**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ**
**КИРОВОГРАДСКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

На правах рукописи
УДК 621.391: 004.7

**МОХАМАД ГАНИ АБУ ТААМ**

# МЕТОД УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫМИ РЕСУРСАМИ ДЛЯ ПОВЫШЕНИЯ ОПЕРАТИВНОСТИ ПЕРЕДАЧИ ДАННЫХ

05. 12. 02 – Телекоммуникационные системы и сети

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель
Смирнов Алексей Анатольевич
доктор технических наук, профессор

Кировоград – 2016

**СОДЕРЖАНИЕ**

# ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ

LLQ – Low Latency Queuing

PPS – Priority Processor Sharing

PSIDDRM – Progressive Suspected-Infected-Detected-Death-Recovered Markov

PSIDDR – Progressive Suspected-Infected-Detected-Death-Recovered

PSIDR – Progressive Suspected-Infected-Detected-Recovered

PSIDRM – Progressive Suspected-Infected-Detected-Recovered Markov

PSIDRT – Progressive Suspected-Infected-Detected-Recovered with Topology

QoS – Quality of Service

RRP – Role Resolution Protocol

RSVP – Resource Reservation Protocol

SEIQR – Suspected-Exposed-Infected-Quarantined-Recovered

SI – Suspected-Infected

SIM – Suspected-Infected Markov

SIR – Suspected-Infected-Recovered

SIRT – Suspected-Infected-Recovered with Topology

SIRM – Suspected-Infected-Recovered Markov

SIT – Suspected-Infected with Topology

SI-WF$^2$Q – Stratified/Interleaved Worst-case Fair Weighted Fair Queueing

SCFQ – Self-Clocked Fair Queuing

VC – Virtual Clock

VFT – Virtual Finish Time

VST – Virtual Start Time

WFQ – Worst-Case Queuing

WFQI – Worst-Case Queuing Improved

WF$^2$Q – Worst-Case Fair Weighed Fair Queuing

ЗПО – злоумышленное программное обеспечение

# ВВЕДЕНИЕ

Экономическое и социальное развитие Украины зависит от выполнения целенаправленной политики широкой информатизации современного общества. Интенсификация инфокоммуникационных отношений является одним из условий приумножения экономического и духовного потенциала страны, совершенствования самосознания ее граждан.

Современный уровень развития телекоммуникационных технологий, их интеграция в глобальные системы и сети позволяет расширить спектр предоставляемых услуг, существенно повысить вычислительные и информационные возможности отдельных локальных и региональных телекоммуникационных систем (ТКС) и эффективность их функционирования. Кардинальные и глубокие изменения в подходах комплексного решения задач эффективного управления ТКС определены законами Украины «Про концепцію Національної програми інформатизації», «Про телекомунікації», постановлением Кабинета Министров Украины «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», и обуславливают актуальность проведения прикладных исследований на пути создания перспективных средств управления телекоммуникационными ресурсами.

Главными особенностями в решении комплекса поставленных задач является наличие ряда внутренних и внешних факторов, существенно повышающих сложность получения результата, а также высокие требования к качеству предоставляемых телекоммуникационных услуг [5, 14, 28, 83, 89, 90, 119]. Это обуславливает использование современных методов и технологий передачи, обработки, кодирования, и хранения данных, механизмов управления и распределения телекоммуникационных ресурсов. [2, 68, 69].

Проведенные исследования показали, что в последнее время наблюдается растущий спрос на облачные вычисления. Так многие известные мировые *IT*-компании анонсировали целый ряд глобальных инициатив, которые призваны помочь клиентам воспользоваться преимуществами облачных вычислений. Эти усилия направлены на дальнейшее расширение облачной системы и позволяют компаниям-партнерам разрабатывать решения и услуги на базе существующих платформ (например, IBM SmartCloud и IBM PureSystems), основанных на открытых стандартах. Поскольку спрос на облачные вычисления среди заказчиков растет, они обращаются к местным поставщикам хостинговых сервисов (Managed Service Providers, MSP) за помощью в усовершенствовании облачных сервисов и повышении их эффективности [84].

В этих условиях возникает необходимость в разработке перспективных методов и механизмов управления телекоммуникационными ресурсами, которые могут повысить оперативность доставки специальных данных сигнатур (метаданных) в облачные вычислительные системы.

В настоящее время для решения данных задач используются различные методы (алгоритмы, процедуры) и средства, реализованные и адаптированные в модели *NGN*, что дает возможность использовать механизмы оптимальной маршрутизации, управления очередями и нагрузкой, распределения доступа к информационным и вычислительным ресурсам [27, 28, 55, 78-125]. Реализация подобных функций в интеллектуальных узлах коммутации позволяла, до недавнего времени, обеспечивать требуемое время передачи данных. Однако повышение спроса на Cloud-услуги и, соответственно, увеличение интенсивности информационных потоков в последнее время затрудняет, а зачастую делает невозможным достижение заданных вероятностно-временных характеристик, что существенно ограничивает возможности использования облачных вычислительных систем.

Возникает противоречие между расширением спектра IT-услуг, растущим спросом на облачные вычисления, увеличением интенсивности информационного потока в ТКС и жесткими требованиями к качеству обслуживания при передаче специальных сигнатур в облачные вычислительные системы (оперативности, достоверности, безопасности).

Проведенные исследования показали, что в указанных условиях наиболее перспективным направлением является разработка и использование методов управления телекоммуникационными ресурсами для повышения оперативности передачи данных в облачные вычислительные системы.

**Актуальность темы.** Теоретические основы современных методов динамического управления телекоммуникационными ресурсами заложены в работах известных ученых: Бертсекас, Галлагер, Клейнрок, Петерс, Саати, Шенон, Конахович и др. теории информации и кодирования, теории массового обслуживания, определены принципы построения, функционирования и управления информационными потоками и очередями в сетях передачи данных, рассмотрены подходы решения широкого круга задач оптимизации информационно-телекоммуникационных структур. Дальнейшее развитие данного направления получено в работах Вегешны, Вишневского, Кучерявого, Назарова, и др. в которых разработаны методы расчета основных вероятностно-временных характеристик сетей передачи данных, исследованы сетевые модели управления информационными потоками и сетевыми ресурсами, что позволило разработать механизмы, алгоритмы и протоколы, повышающие основные показатели качества обслуживания для отдельных приложений и услуг сети связи.

Однако конструктивные методы управления телекоммуникационными ресурсами для повышения оперативности передачи специальных сигнатур в облачные вычислительные системы исследованы недостаточно.

Таким образом, **научно-техническая задача** разработки метода управления телекоммуникационными ресурсами для повышения оперативности передачи данных является актуальной.

**Связь работы с научными программами, планами, темами.** Исследования в диссертационной работе проводились в соответствии со следующими нормативными актами.

1. Концепция Национальной программы информатизации, одобренная Законом Украины «Про Концепцію Національної програми інформатизації» от 4 февраля 1998 г. N 75/98-ВР.

2. Закон України «Про телекомунікації» від 18.11.2003 р. № 1280-IV.

3. Закон України «Про захист в інформаційно-телекомунікаційних системах» від 31.05.2005 р. № 2594-IV.

4. Постанова Кабінету Міністрів України від 29.03.2006 №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» (зі змінами 2006, 2011 рр.).

5. Планы научной и научно-технической деятельности Кировоградского национального технического университета в пределах научно-исследовательских работ: госбюджетная тема № 36Б113 «Разработка методов повышения оперативности передачи и защиты информации в телекоммуникационных системах» (№ госрегистрации 0113U003086); госбюджетная тема № 36Б115 «Разработка методов синтеза тестовых моделей поведения программных объектов, повышения оперативности и защиты информации в телекоммуникационных системах» (№ госрегистрации 0115U003103); «Разработка методов повышения безопасности телекоммуникационных сетей» (№ госрегистрации 0112U006630); «Методы повышения оперативности передачи данных и защиты информации в телекоммуникационной сети» (№ госрегистрации 0112U006631), в которых автор был соисполнителем.

**Цель и задачи исследований.** Цель диссертационного исследования состоит в повышении оперативности передачи данных на основе динамического управления телекоммуникационными ресурсами.

В соответствии с целью работы необходимо решить **научно-техническую задачу**, состоящую в разработке метода управления телекоммуникационными ресурсами для повышения оперативности передачи данных.

Для достижения поставленной цели необходимо решить следующие **частные задачи**:

1. Проанализировать методы и технологии обеспечения качества обслуживания при передаче данных в телекоммуникационных системах, механизмы и средства службы поддержки качества обслуживания, а также исследовать различные подходы математического моделирования ТКС, обосновать выбор направления исследования и формализовать постановку научной задачи разработки метода управления телекоммуникационными ресурсами для повышения оперативности передачи данных.

2. Разработать метод априорной оценки требований оперативности передачи данных в условиях воздействия компьютерных вирусов, на основе математической GERT-модели технологии передачи метаданных в облачные антивирусные системы и математической модели технологии распространения злоумышленного программного обеспечения в ТКС.

3. Разработать математическую GERT-модель технологии передачи метаданных в облачные антивирусные системы, учитывающую показатели реальной надежности и особенности многопутевой маршрутизации.

4. Разработать структурно-логическую GERT-модель технологии распространения компьютерных вирусов, учитывающую фактор возможного выхода из строя телекоммуникационных узлов.

5. Разработать математическую модель технологии распространения злоумышленного программного обеспечения в ТКС, учитывающую ключевую информацию о состояниях телекоммуникационных узлов в процессе деструктивных воздействий компьютерных вирусов, а также фактор использования облачного антивирусного обеспечения в процессе лечения.

6. Разработать метод управления доступом в интеллектуальных узлах коммутации включающий в себя математическую модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета и усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам.

7. Разработать практические рекомендации по применению разработанного метода управления телекоммуникационными ресурсами для повышения оперативности передачи данных.

**Объект исследования**. Процесс повышения оперативности передачи данных в облачные вычислительные системы.

**Предмет исследования**. Метод управления телекоммуникационными ресурсами для повышения оперативности передачи данных.

**Методы исследования.** Исследование процесса передачи специальных сигнатур в облачные вычислительные системы проводилось с использованием теории графов (*GERT*-моделирование). Исследование характера распределения ресурсов в интеллектуальных узлах коммутации ТКС опиралось на основные положения теорий телетрафика и массового обслуживания, а также с учетом особенностей GERT-моделирования. Оценка корректности и достоверности теоретических и практических результатов проводилась с помощью теории вероятностей и математической статистики.

**Научная новизна полученных результатов** обусловлена теоретическим обобщением и новым решением важной научно-технической задачи, состоящей в разработке метода управления телекоммуникационными ресурсами для повышения оперативности передачи данных.

Получены следующие **научные результаты**.

1. **Впервые** разработан метод управления доступом в интеллектуальных узлах коммутации, отличающийся от известных комплексным использованием стандартных критериев управления информационными потоками в интеллектуальных узлах коммутации с дополнительными, учитывающими возможность обслуживания информационных пакетов

метаданных при их передаче в облачные вычислительные системы, что позволило повысить оперативность обслуживания информационных пакетов метаданных в интеллектуальных узлах коммутации при их передаче в облачные вычислительные системы.

2. **Усовершенствована** математическая модель технологии передачи метаданных в облачные вычислительные системы, которая отличается от известных учетом показателей реальной надежности и особенностей многопутевой маршрутизации в соответствии с протоколами сетевого уровня, что позволило определить функцию и плотность распределения вероятностей времени передачи метаданных в облачные вычислительные системы.

3. **Получила дальнейшее развитие** математическая модель технологии распространения злоумышленного программного обеспечения в ТКС, в отличие от известных, учитывающая ключевую информацию о состоянии телекоммуникационных узлов в процессе деструктивных воздействий компьютерных вирусов, а также фактор использования облачного антивирусного обеспечения в процессе лечения, что позволило определить время распространения злоумышленного программного обеспечения в ТКС в условиях появления новых сценариев их деструктивного воздействия.

**Практическое значение полученных результатов** заключается в адаптации процесса управления телекоммуникационными ресурсами к изменениям интенсивности информационного обмена в общем и количества передаваемых специальных сигнатур в частности для повышения оперативности передачи метаданных в облачные вычислительные системы, а также в возможности применения предложенного метода для разработки протоколов управления и информационного обмена с интеллектуальными узлами коммутации ТКС.

Практическая значимость полученных результатов состоит в следующем.

1. Разработано автоматизированное программное средство управления очередями в интеллектуальном узле коммутации, что позволило до 3 раз уменьшить время обслуживания информационных пакетов метаданных в интеллектуальных узлах коммутации при их передаче в облачные антивирусные системы.

2. Разработан программно-аппаратный комплекс для моделирования технологии передачи метаданных в облачные антивирусные системы. Использование полученных с его помощью вероятностно-временных показателей позволило повысить точность оценки времени распространения злоумышленного программного обеспечения до 1,4 раза.

3. Разработано специальное программное и математическое обеспечение для моделирования технологии распространения злоумышленного программного обеспечения в ТКС. Показано, что его использование позволило расширить спектр возможных сценариев их деструктивного воздействия до 30% и сформировать требования к вероятностно-временным показателям локализации и лечения узлов ТКС.

Практическая значимость полученных результатов подтверждается их применением (приложение Б):

– при проектировании системы управления телекоммуникационными ресурсами для повышения оперативности передачи данных, которые передаются по каналам связи интернет-сервис провайдера «ИСП Империал», акт внедрения от 17.04.2015 г.;

– в учебном процессе Кировоградского национального технического университета, акт внедрения от 20.05.2015 г.

**Личный вклад автора.** Все результаты, изложенные в диссертационной работе, получены автором самостоятельно. В работах, выполненных в соавторстве и опубликованных в изданиях, которые вошли в перечень ВАК Украины, автору принадлежат:

– в [32] разработана математическая GERT-модель технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях;

– в [33] разработан метод управления доступом в интеллектуальных узлах коммутации;

– в [34] разработана математическая GERT-модель технологии передачи метаданных в облачные антивирусные системы;

– в [35] разработана структурно-логическая GERT-модель технологии распространения компьютерных вирусов;

– в [36] проведены сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях;

– в [37] разработана математическая модель интеллектуального узла коммутации;

– в [38] исследованы показатели качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях;

– в [39] разработан алгоритм управления доступом к «облачным» телекоммуникационным ресурсам;

– в [40] проведен анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты данных;

– в [41] проведено исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам;

– в [42] разработан метод управления доступом к интеллектуальным коммутационным узлам телекоммуникационных систем и сетей.

**Апробация результатов диссертации.** Основные результаты диссертации докладывались и были одобрены на 12 конференциях [43-54]: научно-практической конференции «Применение информационных технологий в подготовке и деятельности сил охраны правопорядка» (Харьков, 2014, АВВ МВД) [43]; VI и VII международных научно-

практических конференциях «Проблемы и перспективы развития IT-индустрии» (Харьков, 2014, 2015, ХНЭУ) [44, 49]; XVI и XVII международных научно-практических семинарах «Комбинаторные конфигурации и их применение» (Кировоград, 2014, 2015, КНТУ) [45, 50]; научно-практической конференции «Информационные технологии и компьютерная инженерия» (Кировоград, 2014, КНТУ) [46]; научно-практической конференции «Актуальные вопросы обеспечения кибернетической безопасности и защиты информации» (Киев, 2015, ЕУ) [47]; всеукраинской научно-практической конференции «Информационная безопасность государства, общества и личности» (Кировоград, 2015, КНТУ) [48]; II международной научно-практической конференции «Информационная и экономическая безопасность» (INFECO-2015)». (Харьков, 2015, ХИБД УБД НБУ) [51]; XI международной конференции «Стратегия качества в промышленности и образовании» (Варна, 2015, ТУВ) [52]; международной научно-практической конференции «Компьютерные технологии и информационная безопасность» (Кировоград, 2015, КНТУ) [53]; первой всеукраинской научно-практической конференции «Перспективные направления защиты информации» (Одесса, 2015, ОНАЗ) [54].

**Публикации.** По результатам диссертационных исследований опубликовано 23 научных работы, из которых 2 коллективных монографии [32, 33], 9 статей [34-42] (в специализированных научных изданиях, которые входят в научно-метрические базы, из них 1 в зарубежном издании); 12 материалов конференций [43-54].

**Структура и объем диссертации.** Диссертационная работа состоит из введения, четырех разделов, заключения, списка использованной литературы, приложений. Общий объем диссертации составляет 152 страницы Основное содержание изложено на 146 страницах, в том числе 13 таблицах, 28 рисунках. Список использованной литературы содержит 125 наименований. Работа содержит 2 приложения.

# РАЗДЕЛ 1
# АНАЛИЗ И ИССЛЕДОВАНИЕ МЕТОДОВ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫМИ РЕСУРСАМИ ДЛЯ ПОВЫШЕНИЯ ОПЕРАТИВНОСТИ ПЕРЕДАЧИ ДАННЫХ. ОБОСНОВАНИЕ ВЫБОРА НАПРАВЛЕНИЯ ИССЛЕДОВАНИЯ

В данном разделе анализируются перспективные методы и алгоритмы управления телекоммуникационными ресурсами, требования обеспечения качества передачи данных в телекоммуникационных системах, основные направления и подходы математического моделирования, формулируется задача разработки метода управления телекоммуникационными ресурсами для повышения оперативности передачи данных.

## 1.1. Анализ существующих методов и средств обеспечения качества обслуживания при передаче данных в телекоммуникационных системах

Являясь частью инфраструктуры экономики государства, телекоммуникационные системы играют чрезвычайно важную роль в жизни общества и определяют степень его информатизации и интеллектуального развития. В условиях формирования социально и экономически развитого общества, реформирования и пересмотра подходов к форматам и методам управления государственными отраслями и ведомствами этот факт подразумевает повышенное внимание к новейшим разработкам методов и средств обеспечения качества услуг и качества обслуживания при передаче данных в телекоммуникационных системах. Особенно важной данная задача представляется в условиях использования централизованных ресурсов хранения и обработки данных (облачных ресурсов). Рассмотрим основные требования обеспечения качества обслуживания, в соответствии с рекомендациями международных союзов и организаций [74, 119].

### 1.1.1 Анализ требований обеспечения качества передачи данных в телекоммуникационных системах

Проведенные исследования показали, что в соответствии с рекомендациями *E.430, E.800, X.134* и др. международного союза электросвязи под качеством обслуживания (*Quality of Service, QoS*) понимается обобщенный (интегральный) полезный эффект от обслуживания, который определяется степенью удовлетворения пользователя как от полученной услуги, так и от самой системы обслуживания [12, 13, 71, 74].

Критерий *QoS* в телекоммуникационном бизнесе, как правило определяется набором показателей свойств как предоставляемой телекоммуникационной услуги, так и используемых сетевых ресурсов. Показатели качества предоставления услуги называют параметрами *QoS* услуги, а показатели качества сетевых ресурсов – параметрами совершенства сети (*Network Performance, NP*) [26].

Общая схема характеристик и показателей, относящихся к качеству обслуживания и эффективности функционирования телекоммуникационной сети в соответствии с международными рекомендациями (*ITU-T, ETSI, IETF, TL 9000, E.800*) [74, 119] представлена на рис. 1.1.

Для количественной характеристики большинства определённых в рекомендации *TL 9000* и *E.800* свойств качества телекоммуникационных услуг вводятся соответствующие показатели, определяемые на основе рабочих характеристик (параметров) сети.

Анализ рекомендаций *I.350* показал, что качество предоставляемых телекоммуникационных услуг обеспечивается на трех стадиях:

– доступ к передаче информации (установление соединения);

– передача информации пользователя;

– завершение сеанса передачи информации (разъединение соединения).

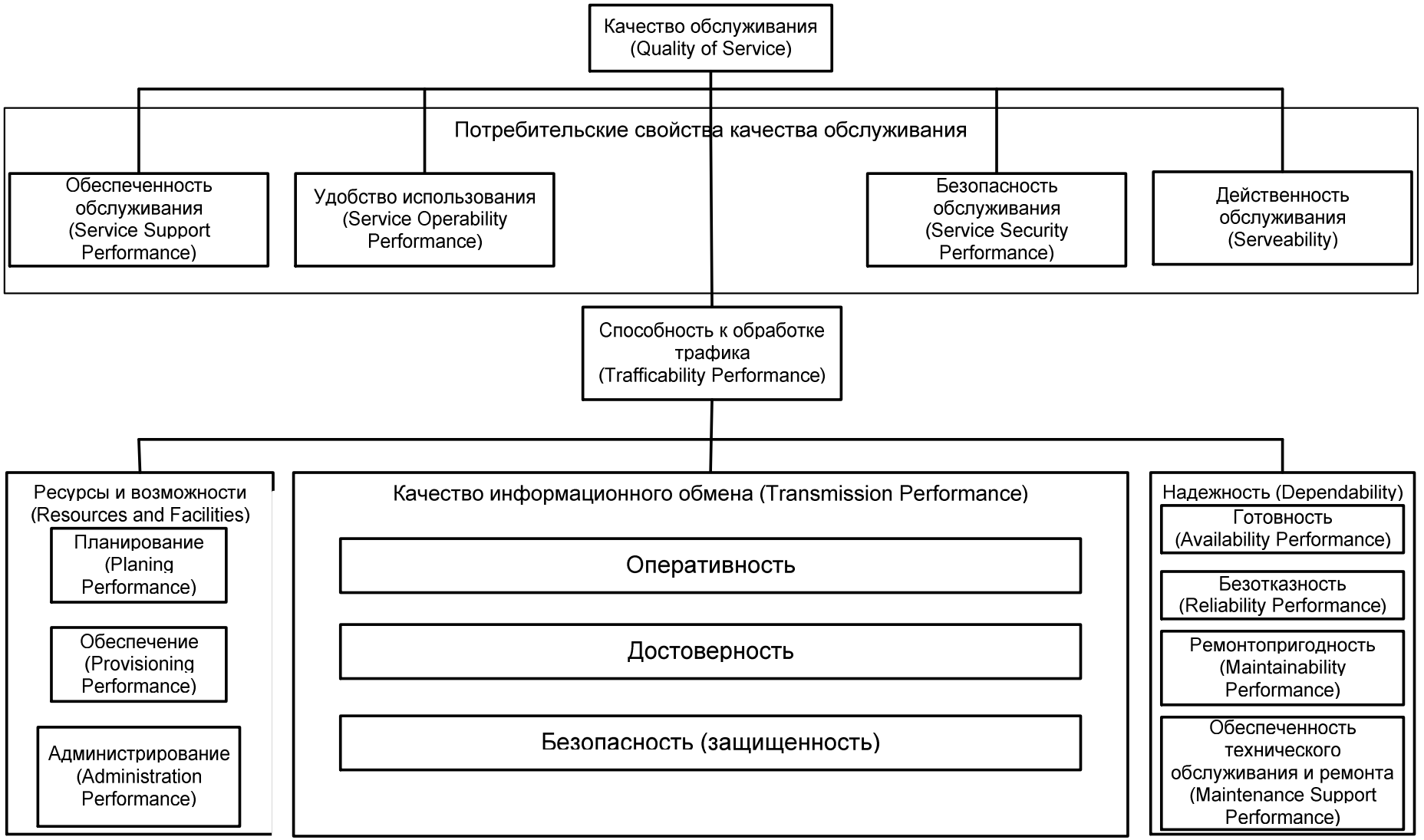



Рис. 1.1. Схема характеристик и показателей, относящихся к качеству обслуживания и эффективности функционирования телекоммуникационной сети

Каждая из частей услуги в свою очередь характеризуется тремя основными показателями, образуя матрицу 3х3 (таблица 1.1):

– оперативность (время установления соединения, время (эффективная скорость) передачи информации пользователя, вероятность своевременной доставки информации пользователя и время разъединения соединения);

– безопасность – это свойство, характеризующее способность системы противостоять случайным или преднамеренным, внутренним или внешним воздействиям, следствием которых могут быть ее нежелательное состояние или поведение (вероятность навязывания ложных соединений, вероятность ввода ложных данных, вероятность ложного завершения работы и др.);

– достоверность (гарантированность установления соединения, передачи данных и разъединения соединения, характеризуемые вероятностью отказа в установлении соединения, вероятностью потери информации пользователя, вероятностью отказа в разъединении соединения и др.).

Таблица 1.1

Основные показатели качества информационного обмена

| Стадии предоставления услуги | Показатели качества | | |
|---|---|---|---|
| | Оперативность | Безопасность | Достоверность |
| Доступ к передаче данных | Время установления соединения | Вероятность навязывания ложных соединений | Вероятность отказа в установлении доступа |
| Передача данных | Скорость передачи данных<br>Время передачи данных<br>Джиттер времени передачи данных | Вероятность ввода ложных данных | Вероятность потери данных |
| Завершение передачи данных | Время разъединения | Вероятность ложного завершения работы | Вероятность отказа в разъединении |

Из литературы [12] известно, что оперативность – это свойство ТКС, характеризующее ее быстродействие при передаче данных.

Как видно из табл. 1.1. одним из показателей оперативности является время $\tau_{пер_i}$ передачи $i$-го информационного пакета.

Основными составляющими времени $\tau_{пер_i}$ являются:

$$\tau_{пер_i} = \tau_{сер_i} + \tau_{к_i} + \tau_{ож_i} + \tau_{расп_i}, \quad (1.1)$$

где:

$\tau_{сер_i}$ – задержка сериализации (*serialization delay*) – время, которое требуется устройству на передачу пакета при заданной ширине полосы пропускания;

$\tau_{к_i}$ – задержка коммутации (*switching delay*) – время, которое требуется устройству, получившему пакет, для начала его передачи следующему устройству. Как правило, это значение меньше 10 нс;

$\tau_{расп_i}$ – задержка распространения (*propagation delay*) – время, которое требуется переданному биту информации для достижения принимающего устройства на другом конце канала;

$\tau_{ож_i}$ – задержка ожидания в очереди – время ожидания на передачу в буфере памяти узлов связи.

Безопасность ТКС – это свойство, характеризующее способность телекоммуникационной сети противостоять случайным или преднамеренным, внутренним или внешним воздействиям, следствием которых могут быть ее нежелательное состояние или поведение. Безопасность достигается применением аппаратных, программных и криптографических методов и средств защиты, а также комплексом организационных мероприятий [14, 28].

В работах [13, 68] представлен такой показатель как безопасное время $T_б$ [*Security time*] – математическое ожидание времени раскрытия системы защиты статистическим апробированием возможных вариантов доступа к

данным. Его можно отнести к перечню ресурсных возможностей телекоммуникационных сетей, задействованных оператором (*Resources and Facilities*), и использовать при анализе ряда злоумышленных атак на ресурсы ТКС. В то же время данный показатель не в полном объеме описывает защищенность системы от атак компьютерных вирусов. Поэтому возникает необходимость введения показателей, характеризующих способность системы противостоять атакам с помощью злоумышленного программного обеспечения. Данный показатель является комплексным, и может быть представлен в виде произведения матриц:

$$B_i^{(ТКС)} = (X_{ik} \cdot Y_k) \cdot A, \qquad (1.2)$$

где $B_i^{(ТКС)}$ – показатель, характеризующий выполнение требований информационной и функциональной безопасности в случае воздействия на систему злоумышленного программного обеспечения, $X_{ik} = \left[ x_{\psi}^{(\xi)} \right]$ – матрица усредненных коэффициентов влияния атак компьютерных вирусов и другого злоумышленного программного обеспечения на отдельные показатели качества обслуживания, $i$ – количество возможных воздействий злоумышленного программного обеспечения, влияющих на функционирование системы, $k$ – количество подсистем ТКС, $x_{\xi}^{(\psi)} = \frac{1}{N} \sum_{j=1}^{N} x_{\ell_j}^{(\psi)}$ – усредненный коэффициент влияния атак компьютерных вирусов и другого злоумышленного программного обеспечения ($\psi$) на показатели качества функционирования отдельных подсистем ТКС ($\xi$), $\ell$ – наименование отдельного показателя качества функционирования подсистемы ТКС, $A$ – матрица усредненных коэффициентов взаимовлияния различных подсистем ТКС в процессе распространения компьютерных вирусов, $Y_k$ – матрица показателей качества в подсистемах ТКС.

Как видно из выражения 1.2. на приведенный показатель безопасности влияют (непосредственно или опосредованно) множество показателей *QoS* (в том числе и время передачи информационных пакетов).

Достоверность – это свойство телекоммуникационной сети, характеризующее способность воспроизведения передаваемых сообщений в пунктах приема с заданной точностью [13]. В сетях, ориентированных на пакетную передачу, основными показателями достоверности являются вероятности правильного приема $P_{пр}$ двоичных символов или их искажения $P_{иск}$ в процессе передачи вида:

$$P_{пр} = \lim_{n_0 \to \infty} \frac{n_1}{n_0} \quad \text{или} \quad P_{иск} = \lim_{n_0 \to \infty} \frac{n_2}{n_0} = 1 - P_{пр},$$

где:

$n_0$ – общее число переданных двоичных символов;

$n_1$ – число правильно принятых двоичных символов;

$n_2$ – число искажений при передаче двоичных символов.

Проведенные исследования показали, что ошибки в общем случае могут привести к различным негативным последствиям, в том числе к отказу абонентов в обслуживании.

Анализ литературы [26, 27] показал, что в настоящее время качество телекоммуникационных услуг сетей связи следующего поколения и *QoS* нормируется в основном рекомендациями *ITU-T* (серия *Y.2xxx*), *ETSI* (*NGN R.1, R.2*), *3GPP/IETF* (концепция *IMS, R.5-R.7*) [74, 119] и частично отечественными руководящими документами [12, 13]. Основным механизмом, регулирующим сквозное качество услуг, в том числе и в сетях связи следующего поколения, является соглашение об уровне обслуживания (*Service Level Agreement, SLA*) между поставщиком (оператором) и пользователем услуг. В общем случае соглашение об уровне обслуживания включает организационно-экономические параметры, а также параметры

производительности сети (скорости передачи данных пользователя), надёжности связи и качества обслуживания передаваемого трафика, которые измеряются путём активного и пассивного тестирования системами поддержки эксплуатации рабочих характеристик сети [26, 27].

Проведенные исследования показали, что в настоящее время *QoS* в ТКС задаётся несколькими способами:

– рекомендациями известных союзов и организаций (Международный союз электросвязи (МСЭ) (таблица 1.1, 1.2 рекомендации МСЭ-*TG.1010* и *TG109* соответственно), Европейский исследовательский центр в области телекоммуникаций (*Research on Advanced Communication in Europe, RACE*) (таблица 1.3, 1.4 рекомендации *RACE*), в терминах сетевой технологии – временем и вероятностью установления соединения, требуемой скоростью передачи, долей потерянных пакетов и пакетов с ошибками, задержкой и вариацией (джиттером) задержки пакетов и др.;

– экспертной оценкой по некоторой шкале, например, по шкале *MOS* (*Mean Opinion Score*);

– классом услуги, которому соответствует набор нормируемых значений её параметров.

Таблица 1.2

Допустимые значения параметров *QoS* при передаче мультимедийного трафика

| Тип сервиса | Параметры *QoS* | | | | |
|---|---|---|---|---|---|
| | Время установления соединения, с. | Вероятность разрыва соединения | Задержка, мс | Джиттер, мс | Вероятность потери данных |
| IP-телефония | 0,5-1 | $10^{-3}$ | 25-500 | 100-150 | $10^{-3}$ |
| Видеоконференция | 0,5-1 | $10^{-3}$ | 30 | 30-100 | $10^{-3}$ |
| Цифровое видео по запросу | 0,5-1 | $10^{-3}$ | 30 | 30-100 | $10^{-3}$ |
| Передача данных | 0,5-1 | $10^{-6}$ | 50-1000 | - | $10^{-6}$ |

Таблица 1.3

Модель требований к качеству обслуживания со стороны пользователя

| | | | | | |
|---|---|---|---|---|---|
| Ошибки данных | Терпимы | Разговор (голос, видео) | Передача сообщений (голос, видео) | Потоки (аудио, видео) | Факсимильные сообщения |
| | Нетерпимы | Команды управления (интерактивные игры) | Транзакции (электронная коммерция) | Передача сообщений, загрузка файлов | Фоновая информация (сетевые новости) |
| | | << 1 с. | 2 с. | 10 с. | >> 10 с. |
| | | Задержка информации | | | |

Таблица 1.4

Требования к качеству услуг, предоставляемых ТКС

| Тип данных | Название услуги | Тип передачи | Требуемая скорость и объем передачи | Параметры качества услуги | | |
|---|---|---|---|---|---|---|
| | | | | Задержка, мс | Джиттер, мс | Вероятность потери данных % |
| Аудио | Телефония | Дуплекс | 4-64 кбит/с | <150 мс (отличное качество); <400 мс (допустимое качество) | <1 мс | <3 |
| | Передача голосовых сообщений | Симплекс | 4-32 кбит/с | <1 с (для воспр.); <2 с (для записи) | <1 мс | <3 |
| | Звуковое вещание | Симплекс | 16-128 кбит/с | <10 с | <<1 мс | <1 |
| Видео | Видеоконференция | Дуплекс | >384 кБ/с | <150 мс (отличное качество); <400 мс (допустимое) | | <1 |
| Данные | Доступ к Интернет (Просмотр WEB-страниц) | Симплекс | 10 кБ | <2 с (отличное качество); <4 с (допустимое) | ненорми-ровано | 0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Передача файлов большого объема | Симплекс | 10 кБ-10 МБ | <15 с (отличное качество); <60 с (допустимое качество) | ненормировано | 0 |
| | Передача неподвижных изображений | Симплекс | 100кБ | <15 с (отличное качество); <60 с (допустимое качество) | ненормировано | 0 |
| | Доступ к серверу электронной почты | Симплекс | <10 кБ | <2 с (отличное качество); <4 с (допустимое качество) | ненормировано | 0 |
| | Факс | Симплекс | 10 кБ | <30 стр/с | ненормировано | $<10^{-6}$ BER |

Следует заметить, что, к сожалению, основные параметры *QoS,* зафиксированные в рекомендациях известных организаций не включают информацию о требованиях к таким данным как специальные сигнатуры (хеш-функции) и другим видам специализированных данных информационного обмена с облачными вычислительными системами (например, облачными антивирусами). Данный факт подтверждает целесообразность дополнительных исследований с целью выявления требований *QoS* при передаче подобного вида данных.

Проведенные исследования показали, что для обеспечения *QoS* на физическом уровне ТКС используются интеллектуальные элементы маршрутизаторов, которые, как правило, выполняют функции основных исполнительных механизмов службы поддержки качества, поскольку именно они оказывают непосредственное влияние на процесс продвижения пакетов между вводными и выводными интерфейсами коммутационного оборудования [26, 27]. Рассмотрим основные технологии обеспечения *QoS* телекоммуникационных ресурсов.

### 1.1.2. Анализ современных технологий обеспечения качества обслуживания

Сети связи следующего поколения (*NGN*) характеризуются открытой архитектурой, что определяет наличие в их составе различных компонентов (уровней, плоскостей) и технологий (*IP, MPLS*, и др.) с адаптивными к требованиям клиентов метриками параметров качества. В данных условиях качество предоставляемых услуг предлагается обеспечивать с использованием интегрированной системы управления ресурсами *NGN*, реализующей концепцию обеспечения гарантированного качества услуг (*Service Assurance*). Это с одной стороны предполагает обеспечение требований пользователей на всех уровнях обслуживания для всех приложений и их трансляцию в параметры, определяющие требуемый уровень качества услуг, а с другой стороны обеспечение наиболее важных показателей и характеристик по умолчанию [79]. К таковым можно отнести и временные показатели передачи данных.

Рассмотрим телекоммуникационные технологии *IP, MPLS*, а также составные методы и средства, предназначенные для построения транспортных сетей *NGN*, и их возможности по обеспечению качества обслуживания при передаче разнородного трафика.

Проведенные исследования технологии и используемых в ней протоколов показали, что ее основными особенностями, определяющими область применения являются следующие [69, 74, 78].

1. Алгоритмы функционирования и управления технологии *IP* не требуют предварительного установления соединения, что уменьшает накладные расходы на сетевом уровне. При этом данная технология изначально проектировалась для передачи пакетов в гетерогенных сетях (рис. 1.2). В соответствии с этим *IP* эффективно функционирует в сетях связи со сложной топологией и оборудованием различных производителей, рационально используя адресное пространство.

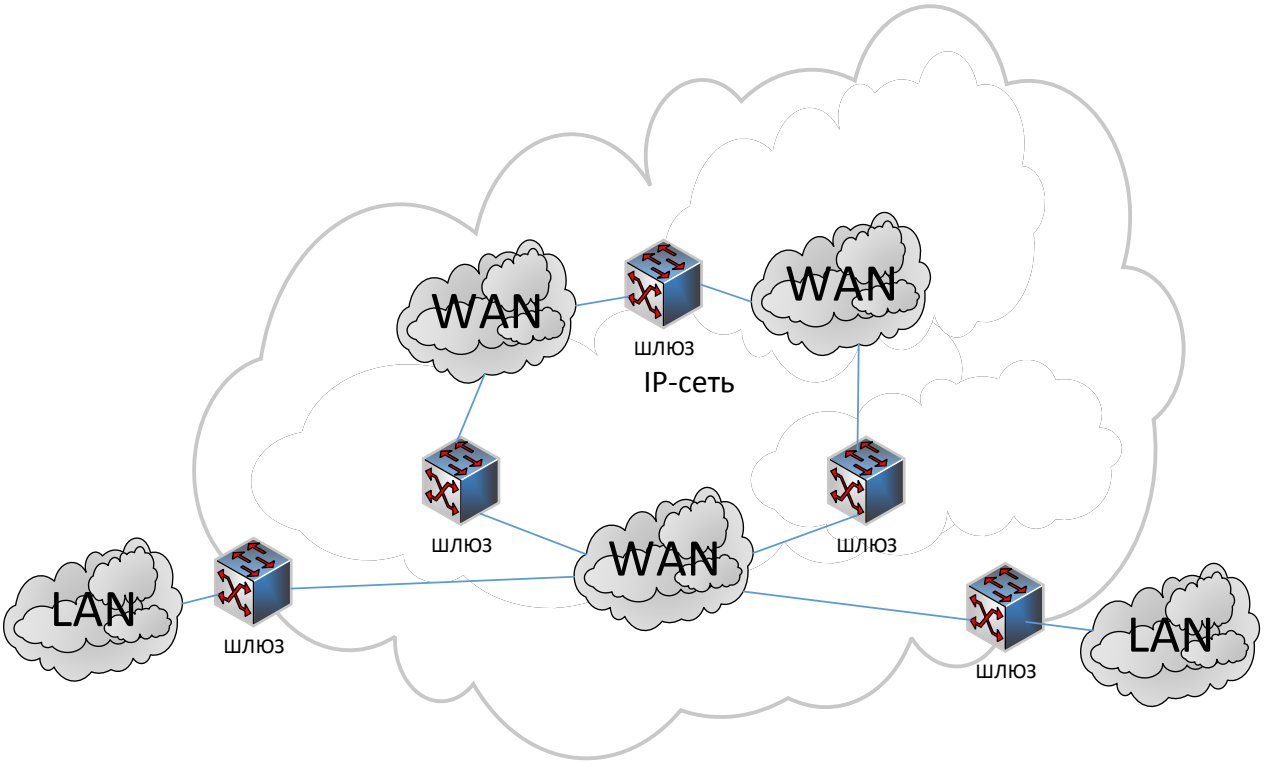



Рис. 1.2. Архитектура IP-сетей

2. Технология *IP* не обеспечивает гарантированной доставки информации и качества обслуживания при передаче в сети, при этом пакеты одного сообщения могут доставляться в сети по различным маршрутам с различной задержкой (джиттером задержки), теряться и изменять порядок следования, что также снижает уровень качества обслуживания и увеличивает вероятность успешного проведения различного рода злоумышленных атак.

3. В данной технологии отсутствуют механизмы управления потоком данных (контроль перегрузок), исправления ошибок и восстановления пропущенных пакетов. Отсутствие данных механизмов требует для обеспечения надёжной доставки данных использования протоколов канального и транспортного уровней.

4. Технология *IP* не предусматривает каких-либо определённых протоколов уровня доступа к среде передаче и физическим средам передачи данных. Требования к канальному уровню ограничиваются наличием интерфейса с модулем *IP* и обеспечением преобразования *IP*-адреса узла

получателя в *MAC*-адрес. В качестве уровня доступа к среде передачи используются технологии *ATM, IPX, X.25* и др.

Перечисленные ограничения технологии *IP* требуют применения дополнительных решений для предоставления услуг реального времени. С этой целью для обеспечения качества обслуживания при передаче разнородного трафика разработаны две взаимодополняющие модели управления трафиком – модели интегрированных (*Integrated Service, RFC 1633*) и дифференцированных (*Differentiated Service, RFC 2475*) услуг, а также внедрены соответствующие протоколы *RSVP, RTCP, RTP,* обеспечивающие управление задержками [86, 90, 112].

Перечисленные технологии в ряде практических случаев позволяют решить задачу обеспечения качества обслуживания отдельных видов телекоммуникационных услуг.

Вместе с тем, практическое применение модели интегрированных услуг обнаружило и её недостатки: жесткая регламентация уровней приоритетности пакетов и соответственно связанные только с данным уровнем гарантии качества обслуживания (это в значительной степени снижает возможности современных протоколов управления ресурсами в обеспечении качества новых услуг связи, в том числе связи с облачными вычислительными системами), низкий уровень масштабирования, а также высокий уровень служебной (сигнальной) информации для контроля состояния соединений и требований к производительности оборудования. Это обуславливает использование данной модели (протоколов) управления трафиком на границах *IP* сети.

Проведенные исследования модели дифференцированных услуг показали, что данная модель является логическим продолжением работ с целью обеспечения динамического качества обслуживания. Основная идея данной модели состоит в предоставлении дифференцированных услуг для набора классов трафика, отличающихся требованиями к показателям

качества обслуживания, определёнными в соглашении об уровне обслуживания (*SLA*).

Следует заметить, что в модели дифференцированных услуг определены два класса (приоритета) услуг: срочное (*Expedited Forwarding, EF, RFC 2598*) [91] и гарантированное продвижение данных (*Assured Forwarding, AF, RFC 2597*) [91], характеризуемые скоростью передачи, задержкой (джиттером) и коэффициентом потери пакетов. С одной стороны данное разбиение в совокупности с относительной простотой классификации трафика, а также отсутствие механизмов сквозного резервирования ресурсов определяют широкое применение модели дифференцированных услуг для обработки интегрированного трафика в мультисервисных сетях связи, но с другой стороны и данная технология не лишена недостатков. В частности модель дифференцированных услуг не позволяет маршрутизировать пакеты, просто игнорируя *DSCP* в их заголовках, и обрабатывать пакеты в соответствии с рядом используемых в ТКС алгоритмов (например, алгоритмом *BE*). Этот факт также может снизить эффективность информационного обмена с облачными антивирусными системами, поскольку удаленное их расположение затрудняет процесс информационного обмена.

Указанные ограничения могут быть устранены путем разработки и применения специальных статических и динамических комбинированных механизмов управления трафиком, позволяющих эффективно распределять ресурсы ТКС. Классификация исследуемых в диссертационной работе приоритетных механизмов управления трафиком, приведена на рис. 1.3.

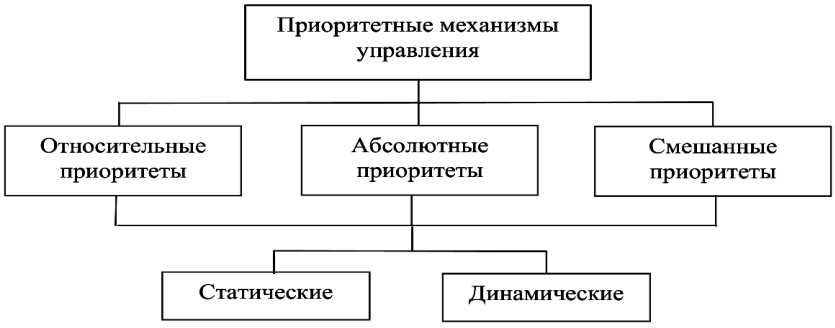



Рис. 1.3. Классификация приоритетных механизмов управления

Проведенные исследования механизмов обеспечения качества технологии *ATM* показали, общую направленность решения задачи в установлении виртуального соединения для каждого информационного потока пользователя.

Анализ данного свойства технологии *ATM* позволил сделать вывод о ее недостатках связанных с отбрасыванием (потерей) низкоприоритетных пакетов при возникновении перегрузок в сети, необходимостью использования высокоскоростного телекоммуникационного оборудования и соответственно высокой стоимостью ее эксплуатации.

Проведенный анализ используемых технологий сетевого и канального уровней показали как их достоинства, так и недостатки. Для объединения достоинств рассмотренных технологий передачи данных разработаны следующие механизмы:

– протоколы передачи *IP* трафика поверх *ATM: Classical IP over ATM (RFC 2225)*, обеспечивающие инкапсуляцию *IP* трафика в ячейки *ATM* на уровне *AAL5* и преобразование адресов для постоянных и коммутируемых виртуальных соединений;

– *Multiprotocol over ATM (MPOA)*, обеспечивающий инкапсуляцию IP трафика в ячейки *ATM* на уровне *AAL5,* маршрутизацию для коммутируемых виртуальных соединений, поддержание параметров трафика и качества обслуживания;

– технология быстрой коммутации пакетов в многопротокольных сетях *MPLS (Multiprotocol Label Switching)*, позволяющая выбирать маршрут передачи на основе идентификационной метки, сопровождающей передачу пакета по сети.

При этом технология *MPLS* предназначена для объединения нескольких сетевых технологий (*ATM, IP*) в рамках единой сети, конструирования трафика (формирования и управления трафиком), создания виртуальных частных сетей (*VPN*), построения высокоскоростных IP-магистралей, а также

магистралей на основе любых других маршрутизируемых сетевых протоколов [78].

Общие рекомендации по применению технологии *MPLS* для решения задач конструирования трафика (*Traffic Engineering, TE*) и обеспечения качества услуг сформулированы в *RFC 2702 "Requirements for Traffic Engineering over MPLS"* [78, 91].

Проведенные исследования показали, что концепция *MPLS* обладает рядом достоинств по сравнению с вышеописанными технологиями *IP* и *ATM*. Это, например, снижение требований к производительности маршрутизаторов, повышение эффективности утилизации каналов, информационной безопасности и биллинга операторов мультисервисной сети за счет децентрализации служб сбора информации о трафике и др.

В то же время и данная технология имеет недостатки, которые могут снизить эффективность функционирования ТКС. Это, например, необходимость контроля параметров *QoS* абонентскими портами совместно с операторами, использование высокопроизводительных, а значит и дорогих, коммутаторов на границе мультисервисной сети, отсутствие детерминированных алгоритмов, с помощью которых определяются значения контролируемых параметров в узлах ТКС и др. Рассмотрим основные механизмы и средства службы поддержки *QoS*.

### 1.1.3. Анализ основных механизмов и средств службы поддержки качества обслуживания

Проведенные исследования показали, что для поддержки *QoS* в настоящее время в телекоммуникационном оборудовании реализованы следующие механизмы [26, 27]:

- кондиционирования трафика;
- управления вводом;

– контроля с обратной связью;
– управления буферами памяти;
– обслуживания очередей.

Исследования механизмов кондиционирования показали, что их реализация позволяет обеспечить эффект «сглаживания» пульсирующего трафика. При этом механизм кондиционирования потока пакетов чаще всего реализуется путем выполнения функций:

– классификации трафика;
– профилирования трафика на основе правил проверки соответствия и обработки;
– формирования трафика;
– ограничения трафика;
– маркирования пакетов в потоке.

Механизмы кондицирования рассчитаны на работу в условиях перегрузок ТКС. Но, к сожалению, они не лишены недостатков. Это в первую очередь формирование задержки пакетов в очередях.

Анализ механизмов управления вводом показал, что они обеспечивают возможность непосредственного контроля характеристик трафика, его классификации и активного влияния на трафик вводного интерфейса с целью недопущения перегрузок элементов сетевого оборудования.

Среди недостатков данного вида механизмов следует отметить невозможность активного влияния на источники нежелательных потоков данных, которые при определенных обстоятельствах могут создать угрозу перегрузок в сети и соответственно потерь информационных пакетов (в том числе неконтролируемых другими средствами ТКС).

Несколько улучшить ситуацию с неконтролируемыми потерями информационных пакетов могут механизмы контроля с обратной связью. Данные механизмы используют обратную связь между узлами ТКС для распространения по сети информации о возникновении перегрузок в ее

элементах. Обратная связь может осуществляться по принципу «из конца в конец» или «шаг за шагом» и выполняться на любом протокольном уровне используемого стека телекоммуникационных протоколов.

Проведенные исследования механизмов управления буферами памяти показали, что основной их целью является определение, когда и какой информационный пакет необходимо отбрасывать для предотвращения возникновения или увеличения степени перегрузки. Среди них можно выделить следующие алгоритмы [26, 27]:

– *TailDrop* – пассивное ограничение очереди;

– *RED* (*Random Early Detection*) – произвольное раннее обнаружение;

– *WRED* (*Weighted RED*) – взвешенное произвольное раннее обнаружение и др.

Их сравнительный анализ позволил выявить ряд недостатков пассивных алгоритмов (*TailDrop*): отсутствие механизмов управления в случае занятия очереди буфера памяти пакетами нескольких информационных потоков, большая зависимость среднего времени доставки информационных пакетов от размера буфера памяти в маршрутизаторе и др.

Анализ алгоритмов активного ограничения очередей (*RED, WRED* и др.). показал, что несмотря на ряд их достоинств (возможность пропорционального отбрасывания информационных пакетов из разных соединений, реализация принципа «справедливого распределения ресурсов») данный класс алгоритмов имеет и недостатки (невозможность заблаговременного определения момента перегрузки буфера памяти и др.).

Проведенные исследования алгоритмов обслуживания очередей позволили выполнить их классификацию, представленную на рис. 1.4.

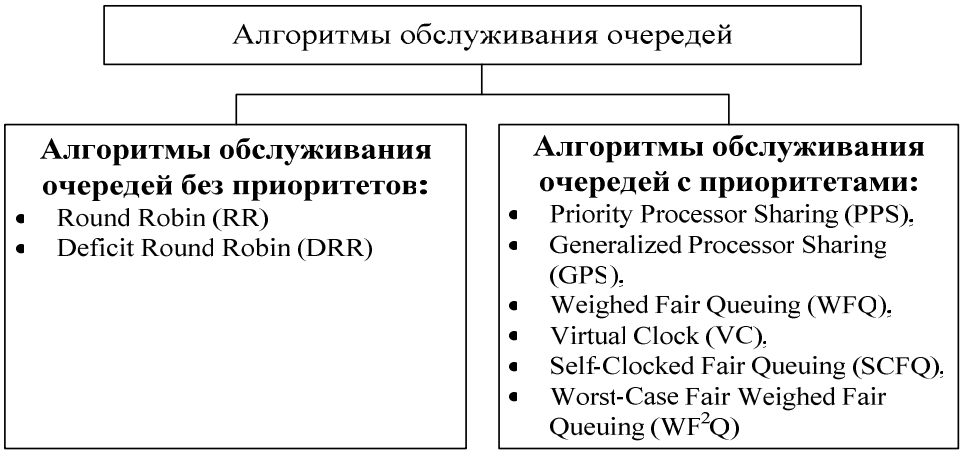



Рис. 1.4. Классификация алгоритмов обслуживания очередей

Сравнительный анализ этих алгоритмов показал, что самыми простыми, с точки зрения, как реализации, так и функционирования являются алгоритмы обслуживания очередей без приоритетов (*RR* (*Round Robin*) и *DRR* (*Deficit Round Robin*)) [26, 66, 69, 70]. В основу указанных алгоритмов положен принцип «циклической очередности» обслуживания, а отличительной их особенностью является то, что в *DRR* добавлена функция накопления квантов выделяемого процессорного времени.

Проведенные исследования показали, что алгоритмы обслуживания очередей без приоритетов имеют ряд общих недостатков, таких как отсутствие гарантий по «справедливому обслуживанию» информационных пакетов различных сетевых служб и переменной длины.

Поэтому на практике все чаще используются алгоритмы обслуживания очередей с приоритетами (*Priority Processor Sharing* (*PPS*), *Generalized Processor Sharing* (*GPS*), *Weighed Fair Queuing* (*WFQ*), *Virtual Clock* (*VC*), *Self-Clocked Fair Queuing* (*SCFQ*), *Worst-Case Fair Weighed Fair Queuing* ($WF^2Q$) и др.) [26, 66, 69, 70].

Как указано в ряде источников [26, 66] основная идея реализации алгоритма *PPS* заключается в том, что каждой из очередей буфера памяти присваивается приоритет. При освобождении процессора планировщик

проверяет очереди на наличие необслуженной нагрузки в соответствии с их приоритетами.

Подобный алгоритм обслуживания очереди имеет такие положительные стороны, как простота реализации и возможность обеспечения низкой задержки для пакетов высокоприоритетного потока. Однако блокировка низкоприоритетного потока информации при постоянном поступлении высокоприоритетного в значительной мере ограничивает возможности маршрутизаторов при обработке мультисервисного трафика.

Для устранения указанных недостатков и осуществления «справедливой» приоритезации доступа планировщика к очередям маршрутизатора был разработан алгоритм *GPS* [66].

В ряде источников [26, 66, 70] отмечено, что для определения времени окончания обслуживания информационных пакетов в системе использующей указанный алгоритм управления используется выражение:

$$F_{i,k} = max\{F_{i,k}, V(t_{(i,k)})\} + L_{(i,k)}, \qquad (1.3)$$

где:

$t_{(i,k)}$ – момент поступления *k*-ого информационного пакета i-ого потока информации;

$L_{(i,k)}$ – длина *k*-ого информационного пакета *i*-ого потока информации;

$V(t_{(i,k)})$ – количество циклов, пройденных планировщиком к моменту $t_{(i,k)}$.

Проведенные исследования показали, что основным достоинством алгоритма *GPS* является возможность изоляции информационных потоков друг от друга (существует возможность «справедливого» обслуживания мультисервисного трафика). Среди ряда его недостатков необходимо отметить отсутствие гарантий по обеспечению требуемого джиттера задержек разнородных потоков информации. Кроме этого из-за того, что алгоритм *GPS*

разрабатывался для систем непрерывного времени его практическая реализация в настоящее время невозможна.

Для устранения указанного недостатка, начиная со второй половины 90-х годов 20-го столетия, на основе алгоритма GPS появляются различные версии алгоритмов обслуживания очередей с приоритетами (*WFQ, $WF^2Q$* и др.) [26, 66, 69, 70].

Исследования алгоритма *WFQ* показали, что для решения задачи управления буфером памяти разработчики несколько видоизменили модель системы планирования, введя новые функции: «виртуального времени поступления» информационного пакета в очередь – $S_{(i,k)}$, и функцию окончания обслуживания – «виртуальное время окончания обслуживания» $\Im_{(i,k)}$. Если предположить, что $\Im_{(i,0)}$=0, то для всех i, имеем:

$$S_{(i,k)} = max\{\Im_{(i,k-1)}, V(t_{(i,k)})\}, \tag{1.4}$$

$$\Im_{(i,k)} = S_{(i,k)} + \frac{L_{(i,k)}}{r_i}. \tag{1.5}$$

Для улучшения функционирования маршрутизаторов и устранения недостатков алгоритмов *GPS* и *WFQ* в 1996 году в [26, 66, 69, 70] была предложена очередная модификация алгоритмов, названная *$WF^2Q$*. Разработчиками этого алгоритма были сформулированы и представлены в виде аналитических выражений общие правила оценки времени обслуживания информационных пакетов в буфере памяти:

$$d_{(i,k)}^{(WF^2Q)} - d_{(i,k)}^{(GPS)} \le \frac{L_{max}}{r}, \tag{1.6}$$

$$W_i^{(GPS)}(0,\tau) - W_i^{(WF^2Q)}(0,\tau) \le L_{max}, \tag{1.7}$$

$$W_i^{(WF^2Q)}(0,\tau) - W_i^{(GPS)}(0,\tau) \le (1-\frac{r_i}{r})L_i, \tag{1.8}$$

где:

$d_{(i,k)}^{(WF^2Q)}$ – время окончания обслуживания *i*-го информационного потока планировщиком $WF^2Q$;

$d_{(i,k)}^{(GPS)}$ – время окончания обслуживания *i*-го информационного потока планировщиком *GPS*;

$W_i^{(WF^2Q)}(0,\tau)$ – количество обслуживания, полученное потоком $i$ за интервал времени $\tau$ в соответствии с алгоритмом $WF^2Q$;

$W_i^{(GPS)}(0,\tau)$ – количество обслуживания, полученное потоком $i$ за интервал времени $\tau$ в соответствии с алгоритмом *GPS*;

$L_{max}$ – максимальная длина информационного пакета *i*-ого потока информации.

На рис. 1.5 приведены примеры обслуживания информационных пактов с помощью алгоритмов *GSP*, *WFQ* и $WF^2Q$ . Из рисунка видно, что после 10 секунд приема в буфер памяти «пачки» из 10 информационных пакетов непосредственно их обслуживание с помощью алгоритма *WFQ* осуществляется в течение последующих 10 секунд.

В то же время дифференцированный подход в обслуживании информационных пакетов, используемый алгоритмом $WF^2Q$ позволяет сглаживать трафик и уменьшать его пачечность.

Однако, как показали исследования [66] проблема обеспечения требуемых временных показателей новых видов трафика с помощью алгоритма $WF^2Q$ не решена.

Своего рода альтернативой приведенным выше алгоритмам *WFQ* и $WF^2Q$ обслуживания очередей в маршрутизаторе являются алгоритмы-планировщики *VC* и *SCFQ* [26, 66].

Как показали исследования, основной отличительной особенностью этих алгоритмов является назначение функциям $V^{VC}(t)$ и $V^{SCFQ}(t)$ «виртуальное

время» значения текущего времени (для *VC*) или времени отправки информационного пакета из системы (для *SCFQ*), т.е.:

$$V^{VC}(t) = t, \ для\ t \geq 0, \tag{1.9}$$

$$V^{SCFQ}(t) = a_{(i,k)}. \tag{1.10}$$

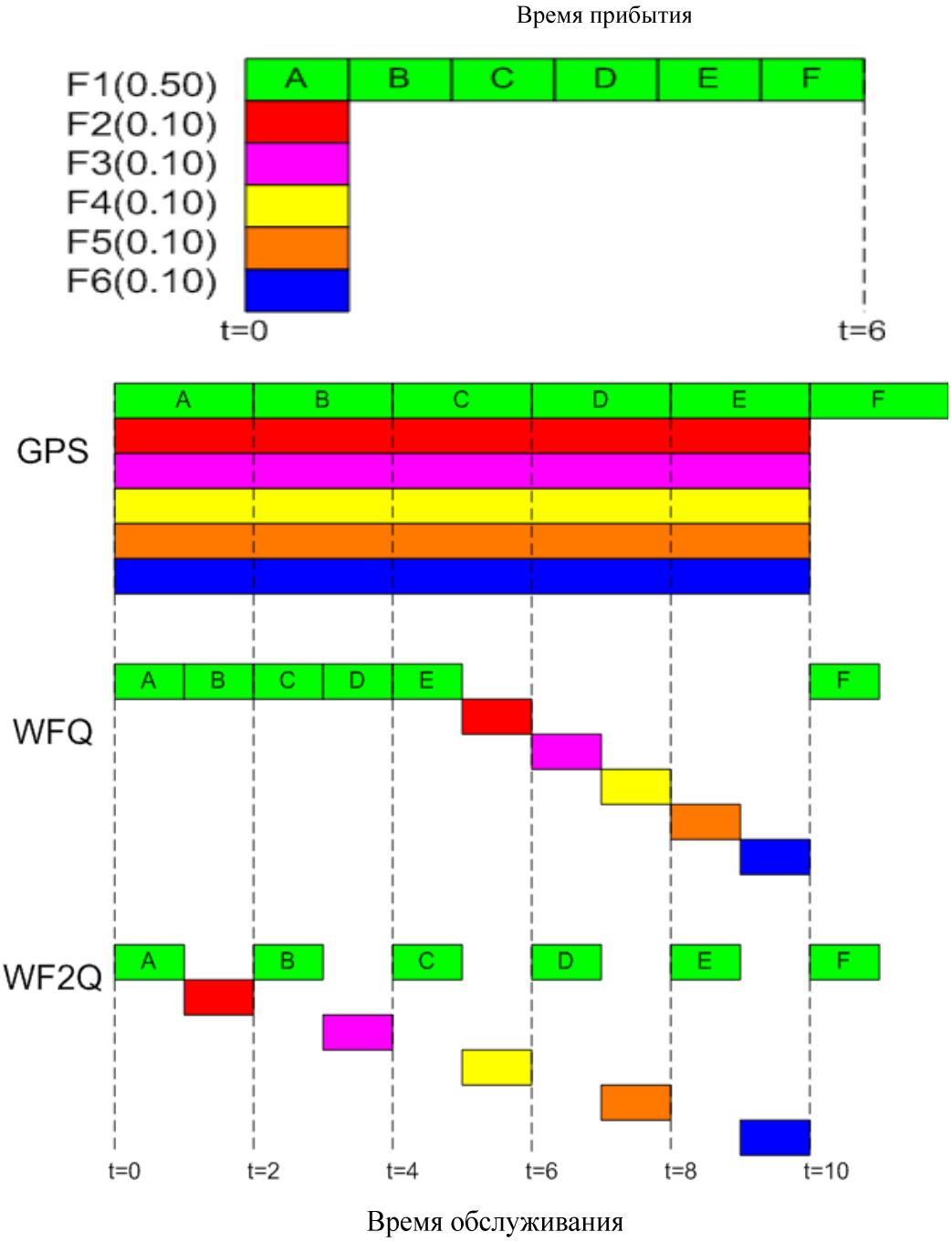



Рис. 1.5. Пример функционирования алгоритмов *GPS*, *WFQ* и $WF^2Q$: порядок ухода пакетов на обслуживание

Тогда, с учетом 1.3, 1.9 и 1.10 можно получить выражение для оценки времени окончания обслуживания информационных пакетов с помощью алгоритмов *VC* и *SCFQ*:

$$F_{i,k} = max\left\{F_{i,k-1}, V^{VC}(t_{(i,k)})\right\} + \frac{L_{(i,k)}}{r_i} = max\left\{F_{i,k-1}, t_{(i,k)}\right\} + \frac{L_{(i,k)}}{r_i}, \quad (1.11)$$

$$F_{i,k} = max\left\{F_{i,k-1}, V^{SCFQ}(a_{(i,k)})\right\} + \frac{L_{(i,k)}}{r_i} = max\left\{F_{i,k-1}, a_{(i,k)}\right\} + \frac{L_{(i,k)}}{r_i}. \quad (1.12)$$

Анализ алгоритмов *VC* и *SCFQ* показал, что основным их достоинством является невысокая вычислительная сложность (*O(logN)*). Однако, как и алгоритмы *WFQ* и *WF2Q* они не обеспечивают требуемых значений времени передачи высокоприоритетных пакетов в условиях высокой загрузки сети.

Сравнительная характеристика возможностей алгоритмов обслуживания очередей с приоритетами представлена в табл. 1.5.

Таблица 1.5

Сравнительная характеристика возможностей алгоритмов обслуживания очередей с приоритетами

| Алгоритм | «Справедливость распределения ресурсов» | Задержка в системе | Вычислительная сложность алгоритма |
|---|---|---|---|
| GPS | соблюдается | $F_{i,k} = \max\{F_{i,k}, V(t_{(i,k)})\} + L_{(i,k)}$ | - |
| WFQ | соблюдается | $S_{(i,k)} = \max\left\{\Im_{(i,k-1)}, V(t_{(i,k)})\right\}$ | O(N) |
| VC | не соблюдается | $F_{i,k} = \max\{F_{i,k-1}, V^{VC}(t_{(i,k)})\} + \frac{L_{(i,k)}}{r_i} = \max\{F_{i,k-1}, t_{(i,k)}\} + \frac{L_{(i,k)}}{r_i}$ | O(logN) |
| SCFQ | соблюдается | $F_{i,k} = \max\{F_{i,k-1}, V^{SCFQ}(a_{(i,k)})\} + \frac{L_{(i,k)}}{r_i} = \max\{F_{i,k-1}, a_{(i,k)}\} + \frac{L_{(i,k)}}{r_i}$ | O(logN) |
| $WF^2Q$ | соблюдается | $d_{(i,k)}^{(WF^2Q)} - d_{(i,k)}^{(GPS)} \le \frac{L_{max}}{r}$, $W_i^{(GPS)}(0,\tau) - W_i^{(WF^2Q)}(0,\tau) \le L_{max}$, $W_i^{(WF^2Q)}(0,\tau) - W_i^{(GPS)}(0,\tau) \le (1 - \frac{r_i}{r})L_i$. | O(N) |

Таким образом, проведенный сравнительный анализ алгоритмов управления очередями показал, что отсутствие механизмов и средств

обеспечения требуемых значений времени передачи высокоприоритетных пакетов в условиях высокой загрузки сети снижает эффективность функционирования приведенных алгоритмов и делает невозможным обеспечение качества обслуживания при передаче высокоприоритетных данных (специальных сигнатур) в облачные вычислительные системы.

Теоретической основой представленным технологиям и механизмам обеспечения качества обслуживания являются математические модели технологии передачи данных. Рассмотрим наиболее известные подходы математического моделирования ТКС.

## 1.2. Анализ и сравнительные исследования подходов математического моделирования ТКС

Проведенный анализ подходов математического моделирования ТКС показал, что в настоящее время существует множество их видов, наиболее результативные из которых базируются на использовании графовых моделей и комбинаторных методов расчета [23, 24, 31, 59, 63, 109], потоковых моделей и методов анализа сетей [6, 7, 17, 61, 62], нейронных сетей [76], тензорных моделей [30] а также аппарата марковских управляемых случайных процессов [1, 4, 8, 15, 27, 29, 60, 70].

Сравнительная характеристика наиболее известных подходов математической формализации технологии передачи данных в ТКС представлена на рис. 1.6.

Как отмечено в ряде источников, доминирующим при решении широкого круга задач анализа и синтеза систем связи различного назначения длительное время оставался графокомбинаторный подход.

В соответствии с методологией теории графов для описания процессов функционирования сетей связи (в том числе и сетей связи следующего поколения) используется функциональное уравнение:

$$W = (X, G), \tag{1.13}$$

где $X = (x_1, \ldots x_n)$ параметры, а $G$ – её структура [31]. При этом под параметром понимается величина, характеризующая свойства сети связи. Различают внутренние (параметры отдельных элементов), внешние (параметры внешней среды, оказывающие влияние на функционирование сети) и выходные (определяющие степень выполнения целевого предназначения) параметры.

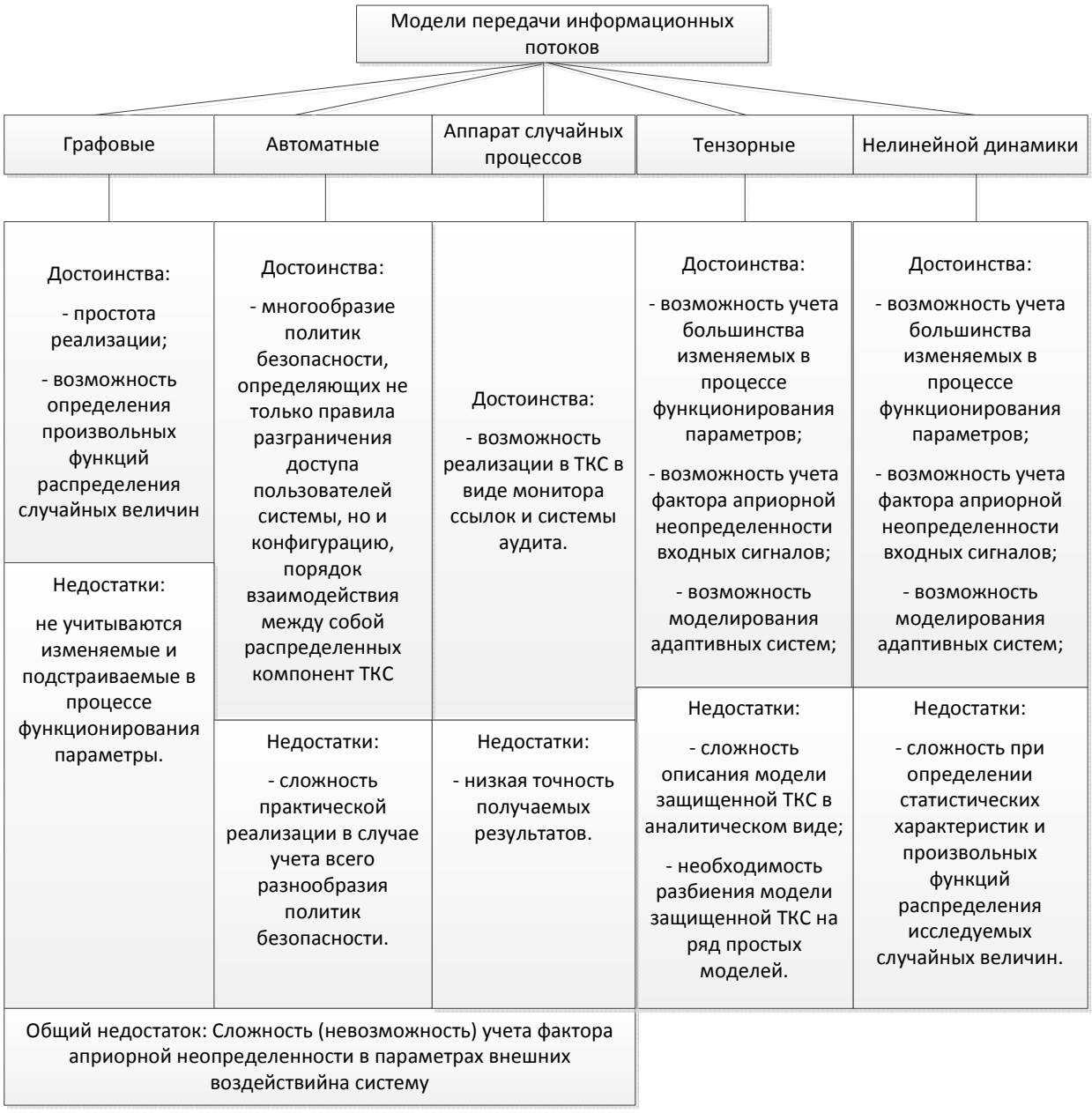



Рис. 1.6. Сравнительная характеристика наиболее известных подходов математической формализации технологии передачи данных в ТКС

В свою очередь структура сети (её морфологическая модель) задается неориентированным графом

$$G = (N, M), \tag{1.14}$$

где $N = \{n_i\}$ – конечное множество вершин (узлов связи – УС), декомпозируемых на совокупность узлов доступа и узлов транспортной сети и характеризуемых координатами их размещения, относительно которых определяются элементы матрицы расстояний между узлами связи $L = \|l_{i,j}\|$, $i, j \in N$; $M = \{m_j\}$ – конечное множество рёбер (сетка линий связи), характеризуемых родом связи и вектором пропускных способностей $V$; $D = N \cup M = \{d_k\}$ – конечное множество элементов графа, где $m_N, m_M, m_D = m_N + m_M$ – число элементов (мощность) множеств *N, M, D*.

Следует заметить, что в теории графов существует ряд отдельных направлений решения задач формализации и оптимизации. Среди них выделим направление *GERT*-моделирования. Данное направление позволяет учесть ряд закономерностей и факторов функционирования ТКС и определить основные статистические характеристики показателей функционирования и качества обслуживания (качества обработки и передачи данных).

Таким образом, проведенные исследования показали объективно существующее противоречие, заключающееся в том, что применяемый математический аппарат, методы управления телекоммуникационными ресурсами, а также средства и механизмы обеспечения качества обслуживания в ТКС не позволяют учесть тенденции развития облачных вычислительных технологий, обеспечить выполнение повышенных вероятностно-временных требований к оперативности, достоверности и безопасности данных в ТКС (см. рис. 1.7).

Следовательно, можно сделать вывод о необходимости разработки и практического использования новых механизмов, методов и средств управления телекоммуникационными ресурсами для повышения оперативности передачи данных в облачные системы.


Рис. 1.7. Объективно существующее противоречие развития методов управления телекоммуникационными ресурсами

## 1.3. Постановка задачи разработки метода управления телекоммуникационными ресурсами для повышения оперативности передачи данных

Долгосрочные перспективы информатизации современного общества, доступность отдельных телекоммуникационных и вычислительных ресурсов широкому кругу абонентов, поэтапный переход от построения узкоспециализированных сетей передачи данных к мультисервисным телекоммуникационным системам, повышение спроса и развитие облачных технологий совместного доступа являются факторами, определяющими дальнейшие направления в развитии целой отрасли телекоммуникационных услуг.

Эффективность выбранной системы зависит от ряда показателей: $\tau_{пер_i}$, $\tau_{ожс_i}$, $B_i^{(ТКС)}$, $P_{пр}$, $P_{иск}$ и др. Как было указано выше, во многом все эти показатели связаны между собой (влияют друг на друга).

В качестве примера можно привести зависимость показателя $B_i^{(ТКС)}$, характеризующего выполнение требований информационной и функциональной безопасности в случае воздействия на систему злоумышленного программного обеспечения от показателя времени передачи специальных сигнатур $T_{пер_{сс}}$ ($T_{пер_{сс}} = \sum_{i=1}^{n} \tau_{пер_i}$) в условиях использования облачных антивирусных систем.

Действительно, именно оперативная передача специальных сигнатур в облачные антивирусные системы позволит обеспечить своевременное обнаружение, локализацию и лечение ТКС и тем самым улучшить показатели безопасности (например, $B_i^{(ТКС)}$). В свою очередь данный показатель непосредственно влияет на показатели достоверности (например, $P_{иск}$). Но и вероятность $P_{иск}$ оказывает влияние на время передачи $T_{пер_{сс}}$ (низкая

вероятность $P_{пр}$ приводит к необходимости частых повторных передач кадров, что в свою очередь увеличивает $T_{пер_{сс}}$). Таким образом, мы видим тесную взаимосвязь между собой показателей качества обслуживания при передаче данных.

Исходя из указанных предположений задачу повышения оперативности передачи данных в облачные вычислительные системы можно представить в виде оптимизационной задачи:

$$T_{пер_{сс}} \to min, \tag{1.15}$$

$$T_{пер_{сс}} = f(\tau_{ож_i}, B_i^{(ТКС)}, P_{пр}, P_{иск}). \tag{1.16}$$

Это требует разработки адекватных математических моделей ТКС, а также усовершенствования метода управления доступом в интеллектуальных узлах коммутации. Исследования должны осуществляться на основе анализа и систематизации уже известных подходов в предметной области ТКС, разработки новых методов стратегического и оперативного синтеза.

Поэтому исследовательскую работу, включающую первый этап, состоящий в изучении проблемы, формировании целей и задач исследования, целесообразно представить в виде структуры проиллюстрированной на рис. 1.8.

Основным методом диссертационного исследования стал системный метод [68], который в отличие от других подразумевает комплексное рассмотрение структурных связей, методов, алгоритмов и процедур, а также протоколов и функций ТКС (структурно-функциональный аспект метода).

Проведенный анализ подходов математического моделирования показал необходимость дальнейших разработок в этой области с целью повышения точности оценки трафика метаданных в ТКС и определения требований оперативности передачи и обслуживания специальных сигнатур для обеспечения антивирусной защиты данных.

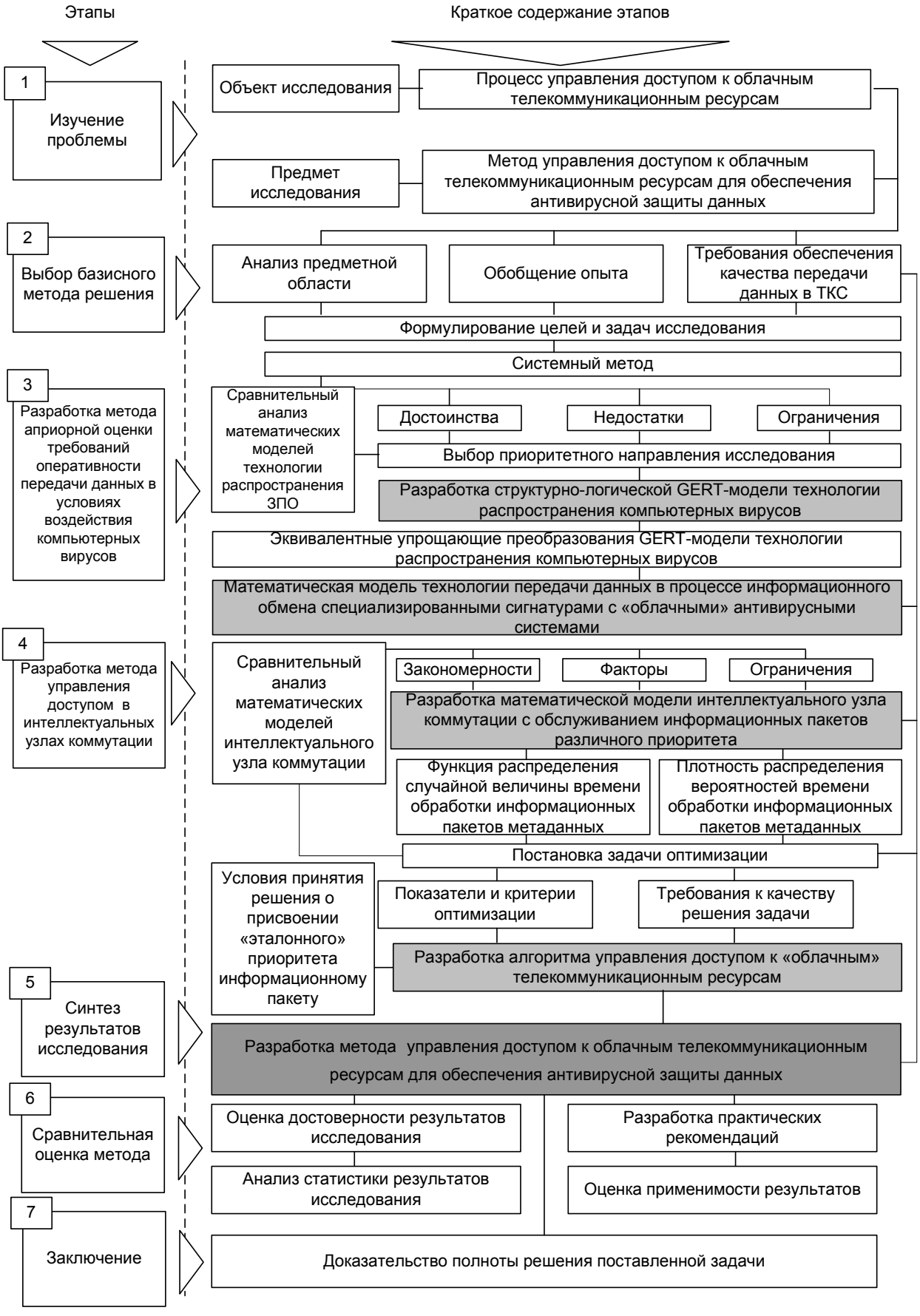



Рис. 1.8. Структурная схема проведения диссертационного исследования

Кроме практической составляющей этого этапа исследования, необходимой для разработки метода управления доступом к облачным телекоммуникационным ресурсам, результаты усовершенствования математической модели технологии передачи данных в процессе информационного обмена специализированными сигнатурами с «облачными» антивирусными системами являются входными данными этапа разработки метода управления доступом в интеллектуальных узлах коммутации.

Проведенный анализ существующих моделей интеллектуального узла коммутации, а так же методов решения оптимизационных задач показал необходимость математического моделирования многопротокольного узла коммутации с обслуживанием информационных пакетов различного приоритета, резервированием ресурсов и учётом реальной надёжности обслуживающих приборов. В основу разработки целесообразно положить положения теории графов и *GERT*-моделирования. Это позволит учесть закономерности распределения ресурсов современного сетевого оборудования (интеллектуальных узлов связи) при передаче различного рода информации (в том числе метаданных), а так же внешние факторы (прежде всего изменения интенсивности входного потока информации), и определить функцию распределения случайной величины времени обработки информационных пакетов метаданных и плотность распределения вероятностей времени обработки информационных пакетов метаданных.

Для решения поставленных в результате моделирования оптимизационной задачи необходимо обладать определенным набором решений, среди которых стоит выделить средства и механизмы обеспечения качества передачи данных реализованные на физическом уровне и уровне доступа модели *NGN*-сети. В частности методы управления очередями буфера памяти интеллектуального узла коммутации. Поэтому на следующем этапе исследования целесообразно разработать алгоритм алгоритма управления доступом к «облачным» телекоммуникационным ресурсам, что

позволит обеспечить требуемые значения оперативности при передаче разнородных потоков данных.

Далее на 5 этапе решается задача синтеза исследования, позволяющая обосновать направления и способы реализации результатов, обобщенно оценивается степень достоверности полученных результатов и определяется их соответствие цели исследования и выдвинутым требованиям.

На следующем этапе исследования, на основании результатов решения задачи оптимизации выносится общее суждение об эффективности разработанного метода, выявляются закономерности, присущие ТКС.

Завершающим этапом исследования (этап 7) является доказательство полноты достижения цели исследования, которое приводит к формулированию заключения по теме.

## Выводы по разделу 1

В разделе проведен анализ основных требований к качеству обслуживания (*QoS*) в ТКС. Выделено, что одними из основных характеристик *QoS* являются оперативность, безопасность, достоверность.

Проведенный анализ и сравнительное исследование существующих методов и средств обеспечения качества обслуживания при передаче данных в телекоммуникационных системах показали, что в условиях использования облачных вычислительных систем в общем процессе обмена данными требования оперативности передачи данных не обеспечиваются. Это подтверждает необходимость дальнейших исследований и разработки метода управления телекоммуникационными ресурсами для повышения оперативности передачи данных в облачные вычислительные системы.

Показано, что одним из определяющих показателей может быть комплексный показатель, характеризующий выполнение требований информационной и функциональной безопасности в случае воздействия на систему злоумышленного программного обеспечения, обеспечение которого

возможно путем разработка и применение новых методов управления ресурсами сетевого оборудования в процессе обмена специальными сигнатурами с облачными антивирусными системами.

Поставлена оптимизационная задача минимизации времени передачи специальных сигнатур в облачные вычислительные системы.

Основные научные результаты, изложенные в первом разделе, опубликованы в работах автора [36, 38, 45, 47].

# РАЗДЕЛ 2
# РАЗРАБОТКА МЕТОДА АПРИОРНОЙ ОЦЕНКИ ТРЕБОВАНИЙ ОПЕРАТИВНОСТИ ПЕРЕДАЧИ ДАННЫХ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

В данном разделе разработан метод априорной оценки требований оперативности передачи данных в условиях воздействия компьютерных вирусов. Основными составляющими метода являются математическая GERT-модель технологии распространения компьютерных вирусов в информационно-телекоммуникационной системе и математическая GERT-модель технологии передачи метаданных в «облачные» антивирусные системы.

Кроме этого в разделе представлены структурно-логическая GERT-модель технологии распространения компьютерных вирусов и методика эквивалентных упрощающих преобразований GERT-модели технологии распространения компьютерных вирусов с возможностью декомпозиции исследуемого объекта на страты.

## 2.1. Математическая GERT-модель технологии распространения компьютерных вирусов в информационно-телекоммуникационной системе

### 2.1.1. Постановка задачи и разработка структурно-логической GERT-модели технологии распространения компьютерных вирусов

В настоящее время в современных ТКС в процессе их эксплуатации возникает множество нештатных ситуаций, обусловленных нестационарностью входной нагрузки, конечной надежностью и отказоустойчивостью ее элементов, внешними дестабилизирующими

воздействиями, требующими автоматических или стационарных управляющих вмешательств в процесс функционирования системы.

Для решения прикладных задач сетевого управления и разработки соответствующих аппаратных или программных средств и приложений остаются актуальными вопросы математического моделирования технологий и процессов сопровождающих информационный обмен (маршрутизации, коммутации, управления и др.). Именно эти вопросы являются одними из наиболее важных и одновременно сложных на этапах проектирования и внедрения ТКС.

Анализ литературы [1- 8, 15, 23, 17, 24, 27- 31, 63, 70, 109] показал, что в настоящее время существует множество подходов и направлений математического моделирования ТКС и компьютерных сетей. Однако большинство задач, возникающих при управлении, оптимизации, тестировании, оценке вероятностно-временных характеристик, параметров надежности, отказоустойчивости, информационной и функциональной безопасности значительно упрощаются, если их рассматривать на теоретико-графовых моделях.

В работах [64-67] проведен анализ и сравнительные исследования основных направлений графового подхода математического моделирования информационно-телекоммуникационных и компьютерных систем и сетей. При этом выявлено, что большинство из указанных выше задач сетевого планирования с минимальной погрешностью можно успешно решить с помощью математического моделирования на основе GERT-сетей.

Разработка графо-аналитических моделей GERT связана с именем американского математика Алана Прицкера [108, 109]. Однако потенциальные возможности математического аппарата GERT-сетей в отдельных направлениях и приложениях современных ТКС в настоящее время еще полностью не использованы.

Проведенные исследования показали, что существует необходимость в усовершенствовании математических моделей технологии распространения

злоумышленного программного обеспечения и антивирусной защиты. Особенно остро эта проблематика выглядит в условиях использования процедур информационного обмена метаданными с «облачными» антивирусными системами для проведения эвристического и сигнатурного анализа, важного в условиях динамически возрастающих угроз злоумышленного программного обеспечения (ЗПО).

В современных условиях динамичного развития информационно-телекоммуникационных технологий все большую важность приобретают программные средства контроля и управления информационными ресурсами. При этом на практике очень часто возникает проблема несанкционированного проникновения в программное обеспечение ТКС путем внедрения ЗПО.

Проведенные исследования [2, 3, 18-23] показали, что в настоящее время существует и постоянно обновляется большое количество подобного рода вредоносных программ, оказывающих значительное влияние на процесс нормального функционирования ТКС. Анализ злоумышленного программного обеспечения позволил представить общую классификацию программных угроз и вредоносного программного обеспечения в виде схемы рис. 2.1.

Как видно из рис. 2.1. такие программы можно разделить на две категории:

– требующие программу-носитель;

– независимые программы.

К первой категории относится программный код, который не может работать независимо от некоторой реальной прикладной программы, утилиты или системной утилиты. Ко второй категории принадлежат самостоятельные программы, которые могут быть запущены стандартными средствами операционной системы, как любая другая программа.

Следует заметить, что хотя классификация, приведенная на рис. 2.1, и позволяет систематизировать информацию о разнородности злоумышленного программного обеспечения, она не дает полного описания реальной картины (например, логические бомбы и "троянские программы" могут быть частями вируса или "червя" и т.д.).

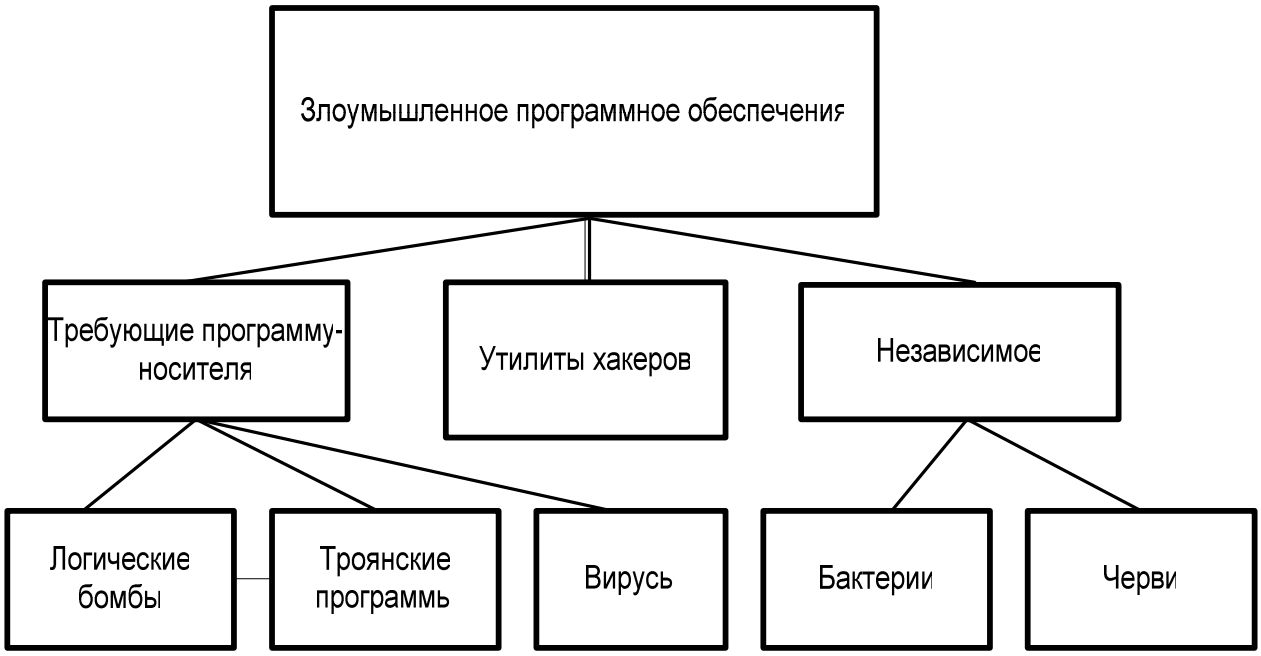



Рис. 2.1. Классификация злоумышленного программного обеспечения

Анализ литературы [18-23], а так же проведенные исследования широкого спектра существующих компьютерных вирусов показали, что наиболее опасными в настоящее время представляются вирусы типа *Flame*. Их отличительной особенностью является наличие множества компонентов кода, функцией которых является выполнение разнообразных вредоносных действий: размножение в сетях различных типов с использованием различных протоколов, похищение и уничтожение конфиденциальной информации, вывод из строя компьютерных систем, шпионаж, взаимодействие с злоумышленным программным обеспечением другого типа и т. д.

Исследования компьютерных вирусов типа *Flame* позволили выделить основные этапы технологии их распространения в ТКС и проиллюстрировать ее структурно-логическую модель в виде диаграммы переходов, представленной на рис. 2.2.

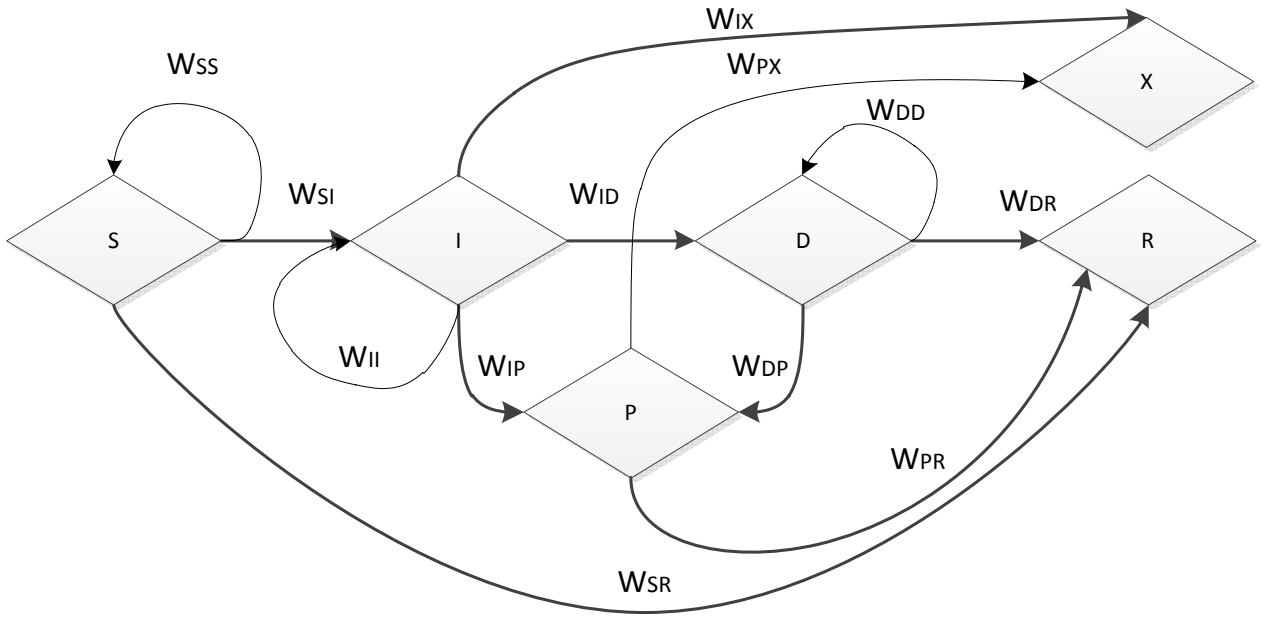



Рис. 2.2. Структурно-логическая GERT-модель технологии распространения компьютерных вирусов типа *Flame*

Как видно из этого рисунка процесс функционирования оконечного оборудования (узлов) ТКС в условиях распространения исследуемого типа компьютерных вирусов можно представить в виде совокупности состояний:

– телекоммуникационные узлы заражены *(I)*;

– телекоммуникационные узлы не заражены *(S)*;

– телекоммуникационные узлы вылечены и обладают иммунитетом *(R)*;

– зараженные телекоммуникационные узлы с выявленным компьютерным вирусом *(D)*;

– в результате действий злоумышленного программного обеспечения телекоммуникационные узлы полностью вышли из строя *(X)*;

– в результате действий злоумышленного программного обеспечения телекоммуникационные узлы частично вышли из строя *(P)*.

Представленная на рис. 2.2. модель может быть описана следующим образом. Ветвь $S \to I$ $(W_{SI})$ интерпретирует процесс проникновения компьютерного вируса в незараженный *k*-й компьютер с вероятностью $P_{зар}^{(k,s^{(i)})}$ в некотором исходном состоянии ТКС $s^{(i)}$. Ветвь $S \to R$ $(W_{SR})$ описывает процесс иммунизации незараженного *k*-го компьютера в исходном состоянии с вероятностью иммунизации $P_{им}^{(k,s^{(i)})}$. Ветвь $S \to S$ $(W_{SS})$ интерпретирует процесс нормального функционирования системы (без заражения) с вероятностью $\left(1 - P_{зар}^{(k,s^{(i)})} - P_{им}^{(k,s^{(i)})}\right)$. Ветвь $I \to D$ $(W_{ID})$ характеризует процесс детектирования зараженного *k*-го компьютера в некотором исходном состоянии ТКС $s^{(i)}$ с вероятностью $P_{дет}^{(k,s^{(i)})}$. Ветвь $I \to X$ $(W_{IX})$ описывает процесс полного выведения из строя *k*-ого узла с вероятностью $P_{вис}^{(k,s^{(i)})}$. Ветвь $I \to P$ $(W_{IP})$ интерпретирует процесс частичного выведения *k*-ого узла из строя с вероятностью $P_{чвис}^{(k,s^{(i)})}$. Ветвь $I \to I$ $(W_{II})$ предусматривает возможность ситуации, когда узел телекоммуникации останется зараженным с вероятностью $\left(1 - P_{дет}^{(k,s^{(i)})} - P_{вис}^{(k,s^{(i)})} - P_{чвис}^{(k,s^{(i)})}\right)$. Ветвь $D \to R$ $(W_{DR})$ описывает процесс лечения зараженного *k*-го компьютера в некотором состоянии ТКС $s^{(i)}$ с вероятностью $P_{леч}^{(k,s^{(i)})}$. Ветвь $D \to P$ характеризует процесс частичного выхода из строя оборудования после того как злоумышленное программное обеспечение типа *Flame* обнаружено. При этом вероятность такого перехода равна $P_{чв}^{(k,s^{(i)})}$. Ветвь $D \to D$ $(W_{DD})$ предусматривает возможность ситуации, когда телекоммуникационный узел выявит злоумышленное программное

обеспечение типа *Flame*, но при этом процесса иммунизации не произойдет (обнаружение с помощью только эвристического анализатора). При этом вероятность такого перехода состояния равна $\left(1 - P_{леч}^{(k,s^{(i)})} - P_{чв}^{(k,s^{(i)})}\right)$. Ветвь $P \rightarrow R$ $(W_{PR})$ интерпретирует процесс восстановления нормального работоспособного состояния и иммунизации оборудования после ситуации частичного выхода из строя. Вероятность такого события в некотором состоянии ТКС $s^{(i)}$ равна $P_{лечв}^{(k,s^{(i)})}$. Ветвь $P \rightarrow X$ $(W_{PX})$ описывает процесс полного выхода из строя зараженного телекоммуникационного оборудования с вероятностью $\left(1 - P_{лечв}^{(k,s^{(i)})}\right)$.

Следует заметить, что для упрощения разрабатываемой GERT-модели принято решение не рассматривать остальные переходы в связи с поставленными при моделировании ограничениями («состояние «выведенный из строя» – конечное состояние объекта», «иммунизированный узел конечная точка модели», «незараженный узел не может быть выведен из строя», «процесс лечения и иммунизации без предварительного детектирования не предусмотрен»), при этом предполагается, что вероятность переходов $R \rightarrow R$ и $X \rightarrow X$ равна единице, а вероятности оставшихся переходов равны нулю.

Указанные выше допущения и ограничения позволили сформировать матрицу вероятностей переходов из одного состояния в другое и представить ее в виде рис. 2.3.

В дальнейшем данный подход позволит сформулировать и представить ряд допущений, ограничений и входных данных для разработки имитационной модели технологии распространения компьютерных вирусов в ТКС.

Анализ ряда работ [1, 23, 24, 67], а также проведенные исследования процесса передачи данных в ТКС позволили сформировать характеристики

рассмотренных в GERT-модели ветвей и параметры распределения и представить их в табл. 2.1.

$$
\begin{array}{c|cccccc}
 & S & I & D & P & R & X \\
S & \left(\begin{array}{l}1 - \\ - P_{зар}^{(k,s^{(i)})} - \\ - P_{им}^{(k,s^{(i)})}\end{array}\right) & P_{зар}^{(k,s^{(i)})} & 0 & 0 & P_{им}^{(k,s^{(i)})} & 0 \\
I & 0 & \left(\begin{array}{l}1 - \\ - P_{дет}^{(k,s^{(i)})} - \\ - P_{вис}^{(k,s^{(i)})} - \\ - P_{чвис}^{(k,s^{(i)})}\end{array}\right) & P_{дет}^{(k,s^{(i)})} & P_{чвис}^{(k,s^{(i)})} & 0 & P_{вис}^{(k,s^{(i)})} \\
D & 0 & 0 & \left(\begin{array}{l}1 - \\ - P_{леч}^{(k,s^{(i)})} - \\ - P_{чв}^{(k,s^{(i)})}\end{array}\right) & P_{чв}^{(k,s^{(i)})} & P_{леч}^{(k,s^{(i)})} & 0 \\
P & 0 & 0 & 0 & 0 & P_{лечв}^{(k,s^{(i)})} & \left(\begin{array}{l}1 - \\ - P_{лечв}^{(k,s^{(i)})}\end{array}\right) \\
R & 0 & 0 & 0 & 0 & 1 & 0 \\
X & 0 & 0 & 0 & 0 & 0 & 1
\end{array}
$$

Рис. 2.3. Матрица вероятностей переходов между состояниями в соответствии с GERT-моделью технологии распространения компьютерных вирусов типа *Flame*

В соответствии с характеристиками ветвей GERT-сети эквивалентную *W*-функцию времени распространения в ТКС компьютерных вирусов типа *Flame* с конечным результатом лечения и иммунизации узлов ТКС можно представить как:

$$W_E(s) = \frac{W_{SI}W_{ID}W_{DR} + W_{SI}W_{IP}W_{PR} + W_{SI}W_{ID}W_{DP}W_{PR} + W_{SR}}{1 - W_{SS} - W_{SI}W_{II} - W_{SI}W_{ID}W_{DD}} =$$

$$= \frac{\left( p_1(\lambda_2/\lambda_2 - s)(\lambda_8/\lambda_8 - s)\begin{pmatrix} p_4 p_8(\lambda_4/\lambda_4 - s) + p_5 p_9(\lambda_5/\lambda_5 - s) + \\ + p_4 p_7 p_9(\lambda_4/\lambda_4 - s)(\lambda_5/\lambda_5 - s) \end{pmatrix} \right)}{\left( \begin{array}{l} 1 - (1 - p_1 - p_2)(\lambda_1/\lambda_1 - s) - p_1(\lambda_2/\lambda_2 - s) \times \\ \times \left( \begin{array}{l} (1 - p_4 - p_5 - p_6)(\lambda_7/\lambda_7 - s) + \\ + (p_4(1 - p_7 - p_8)(\lambda_4/\lambda_4 - s)(\lambda_9/\lambda_9 - s)) \end{array} \right) \end{array} \right)}. \quad (2.1)$$

Таблица 2.1

Характеристики ветвей модели

| № п/п | Ветвь | *W*-функция | Вероятность | Производящая функция моментов |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| 1. | *(S,S)* | $W_{SS}$ | $1 - p_1 - p_2$ | $\lambda_1/(\lambda_1 - s)$ |
| 2. | *(S,I)* | $W_{SI}$ | $p_1$ | $\lambda_2/(\lambda_2 - s)$ |
| 3. | *(S,R)* | $W_{SR}$ | $p_2$ | $\lambda_3/(\lambda_3 - s)$ |
| 4. | *(I,D)* | $W_{ID}$ | $p_4$ | $\lambda_4/(\lambda_4 - s)$ |
| 5. | *(I,P)* | $W_{IP}$ | $p_5$ | $\lambda_5/(\lambda_5 - s)$ |
| 6. | *(I,X)* | $W_{IX}$ | $p_6$ | $\lambda_6/(\lambda_6 - s)$ |
| 7. | *(I,I)* | $W_{II}$ | $1 - p_4 - p_5 - p_6$ | $\lambda_7/(\lambda_7 - s)$ |
| 8. | *(D,P)* | $W_{DP}$ | $p_7$ | $\lambda_5/(\lambda_5 - s)$ |
| 9. | *(D,R)* | $W_{DR}$ | $p_8$ | $\lambda_8/(\lambda_8 - s)$ |
| 10. | *(D,D)* | $W_{DD}$ | $1 - p_7 - p_8$ | $\lambda_9/(\lambda_9 - s)$ |
| 11. | *(P,R)* | $W_{PR}$ | $p_9$ | $\lambda_8/(\lambda_8 - s)$ |
| 12. | *(P,X)* | $W_{PX}$ | $1 - p_9$ | $\lambda_6/(\lambda_6 - s)$ |

Эквивалентную *W*-функцию времени распространения в ТКС компьютерных вирусов типа *Flame* с конечным результатом выхода узлов ТКС из строя можно представить как:

$$W_E(s)=\frac{W_{SI}W_{IX}+W_{SI}W_{IP}W_{PX}+W_{SI}W_{ID}W_{DP}W_{PX}}{1-W_{SS}-W_{SI}W_{II}-W_{SI}W_{ID}W_{DD}}=$$

$$=\frac{p_1(\lambda_2/\lambda_2-s)\begin{pmatrix}p_6(\lambda_6/\lambda_6-s)+\\+(1-p_9)(\lambda_5/\lambda_5-s)(\lambda_6/\lambda_6-s)(p_5+p_4(\lambda_4/\lambda_4-s))\end{pmatrix}}{1-(1-p_1-p_2)(\lambda_1/\lambda_1-s)-p_1(\lambda_2/\lambda_2-s)\times}\cdot \quad (2.2)$$

$$\times\begin{pmatrix}(1-p_4-p_5-p_6)(\lambda_7/\lambda_7-s)+\\+(p_4(1-p_7-p_8)(\lambda_4/\lambda_4-s)(\lambda_9/\lambda_9-s))\end{pmatrix}$$

Следует заметить, что рассматриваемая на рис. 2.2. GERT-сеть, описывает технологию распространения злоумышленного программного обеспечения на высоком уровне стратификации [68]. В этой связи эквивалентная *W*-функция времени распространения в ТКС компьютерных вирусов исследуемого типа представляется с одной стороны достаточно сложной для анализа, а с другой стороны в связи с введенными ограничениями моделирования (выбрана однотипная производящая функция моментов, ветви $W_{IX}$, $W_{PX}$, так же как и ветви $W_{DR}$, $W_{PR}$, а также $W_{DP}$, $W_{IP}$ характеризуются одним и тем же параметром распределения и др.) точность результатов не отвечает выдвигаемым требованиям.

Анализ ряда работ [63, 68] показал, что в этой ситуации для устранения указанных недостатков целесообразно сузить область определения разрабатываемой математической модели путем декомпозиции и эквивалентных упрощающих преобразований.

### 2.1.2. Эквивалентные упрощающие преобразования GERT-модели технологии распространения компьютерных вирусов

Проведенные исследования показали, что использование наиболее известного подхода декомпозиции общей задачи математического моделирования на ряд частных задач в большинстве случаев позволяет решить поставленные задачи с заданной точностью. Однако в некоторых случаях простое использование метода декомпозиции не позволяет достичь

необходимого уровня вычислительной сложности. Поэтому в диссертационной работе для решения задачи математического моделирования технологии распространения компьютерных вирусов типа *Flame* с помощью GERT-сетей предлагается комплексное использование подходов декомпозиции и эквивалентных упрощающих преобразований.

Для этого можно воспользоваться методикой, представленной в работах [63, 65, 68]. В соответствии с этой методикой первым шагом математического GERT-моделирования является декомпозиция рассматриваемого объекта на страты и выбор из них наиболее проблемной области исследования.

Проведенные исследования показали, что процесс стратификации GERT-модели выбранной проблемной области является во многом субъективным, и только разработчик, исходя из своего понимания цели моделирования, может определить уровни детализации, число и взаимосвязи элементов. Для процесса функционирования ТКС в ходе выявления, лечения и иммунизации компьютерных вирусов типа *Flame* рекомендуется определить следующее разбиение на страты.

1) $K$ -страта. Низкоуровневые алгоритмы обработки данных: алгоритмы формирования сигнатур (хеширования и др.); алгоритмы сигнатурного и эвристического анализа (с помощью сетей Маркова, нечеткой логики и др.); алгоритмы скремблирования и помехоустойчивого кодирования (придание потоку битовой информации свойств псевдослучайной последовательности); алгоритмы проверки целостности информации и др.

2) ($K$ +1)-страта. Механизмы обеспечения требуемого уровня качества обслуживания (*QoS*).

3) ($K$ +2)-страта. Низкоуровневое моделирование каналов связи ТКС путем задания их типов, и параметров необходимых для выполнения поставленной задачи (например, пропускной способности, времени задержки распространения и др.) [24, 26].

4) ($K$+3)-страта. Моделирование каналов связи среднего уровня (с учетом специфики разбиения данных на информационные пакеты и кадры). При этом параметрами, необходимыми для выполнения поставленной задачи могут быть минимальный и максимальный размер информационного пакета (кадра), вероятности ошибки в информационном пакете (кадре), время доставки информационного пакета и др. [68].

5) ($K$+4)-страта. Моделирование протоколов и средств передачи данных выполняющих транспортные функции и функции доставки сообщений между конечными узлами (например, *TCP* или *UDP* [57, 58]), коммуникационных протоколов транспортного уровня, протоколов маршрутизации уровня доступа (например, *OSPF, RIP, BGP* и др. [57]).

6) ($K$+5)-страта. Моделирование приложений с помощью команд нескольких типов, в том числе команд обработки данных, отправки и чтения сообщений, чтения и записи данных в файл, установления сессий и приостановки программы до получения сообщений. Для каждого приложения задается так называемый репертуар команд [56].

7) ($K$ + 6)-страта. Моделирование информационного трафика различных сетевых служб с учетом характерных особенностей, основных показателей и законов распределения искомых случайных величин.

8) ($K$+7)-страта. Моделирование сетей на самом верхнем уровне абстракции. Укрупненное моделирование сетей с коммутацией пакетов (например, *TCP/IP* [57]), сетей с коммутацией ячеек (например, *ATM* [55]), сетей с коммутацией меток (например, *MPLS* [125]) и др. При этом каждый тип глобального сервиса характеризуется рядом специфических параметров, таких как минимальный и максимальный размер кадра, и необходимые ресурсы для передачи служебной информации и др.

Анализ процессов протекающих в ТКС показал, что в условиях внешних деструктивных воздействий компьютерных вирусов типа *Flame* одними из основных этапов, позволяющих достичь состояния $R$ (см. рис. 2.2) (телекоммуникационные узлы вылечены и обладают иммунитетом) являются

этапы выявления, лечения и иммунизации злоумышленного программного обеспечения. Проведенные исследования показали, что математическую формализацию указанного процесса целесообразно представить на ($K$+4) уровне стратификации.

Особенно важным данный уровень стратификации представляется при математическом описании процессов выявления, лечения и иммунизации с помощью облачных антивирусных систем, поскольку именно на этом уровне возможен учет основных протоколов передачи данных транспортного (*TCP*, *UDP)* и сетевого *(OSPF, RIP, BGP* и др.) уровней.

Процедура эквивалентного упрощающего преобразования GERT-сети к эквивалентной дуге представляется набором элементарных операций преобразования, в результате которых можно получить эквивалентные характеристические функции. Общая методика эквивалентного упрощающего преобразования *GERT*-сети а также основные математические выкладки, характеризующие данную методику представлены в работах [63, 68].

Схема алгоритма эквивалентного преобразования GERT-сети представлена на рис. 2.4.

Отличительной особенностью данного алгоритма является введение процедур определения внутренних одноуровневых подсетей и исключения петель первого рода.

Проведенные исследования показали соизмеримость результатов моделирования эквивалентной GERT-сети с первоначальной структурой. Именно это позволило провести математическое моделирование и анализ компьютерных вирусов типа *Flame*, и сделать вывод о том, что подход, основанный на GERT-моделировании, позволяет учесть ряд деструктивных факторов, присущих данному типу вирусов, и тем самым расширить спектр возможных сценариев деструктивных воздействий до 30%.

Воспользуемся описанной в данном подразделе методикой эквивалентных упрощающих преобразований, для математической

формализации технологии передачи данных в процессе информационного обмена специализированными сигнатурами с «облачными» антивирусными системами.

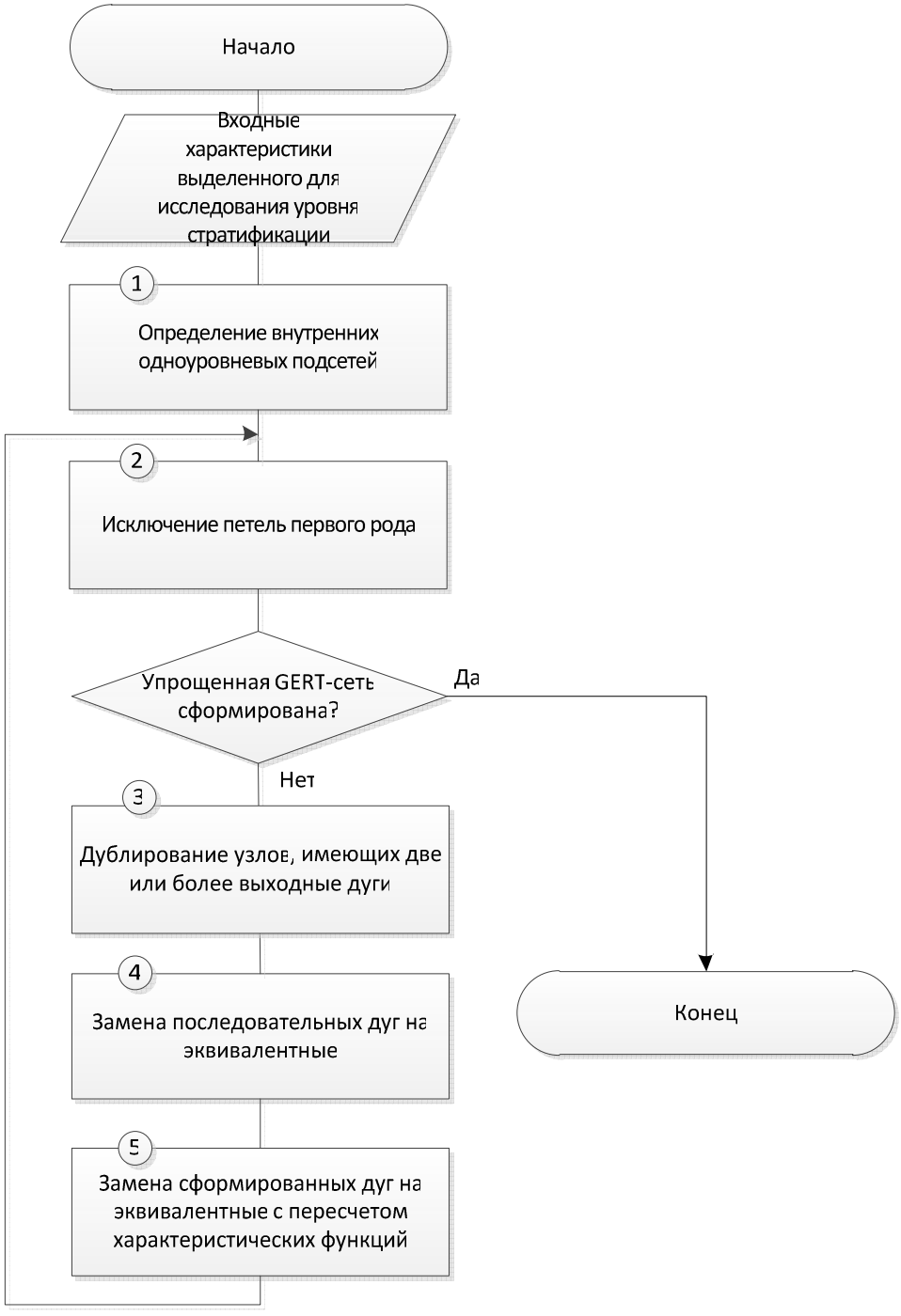



Рис. 2.4. Схема алгоритма эквивалентного преобразования GERT-сети

## 2.2. Математическая модель технологии передачи данных в процессе информационного обмена специализированными сигнатурами с облачными антивирусными системами на основе GERT-сети.

В последнее время у пользователей ТКС все большим спросом пользуются услуги «облачных» антивирусных систем. Связано это во многом с одной стороны с динамическим развитием сетевых технологий, а с другой, ростом реальных угроз компьютерных вирусов, справиться с которым стационарные антивирусные системы не в состоянии [114].

Процесс информационного обмена оконечных рабочих станций с узлами, предоставляющими услуги «облачной» антивирусной защиты, представляет собой четко организованную функциональную структуру, являющуюся совокупностью алгоритмов формирования сигнатур, транспортировки, коммутации, маршрутизации и обработки специализированными анализаторами. Обобщенная структура и временная диаграмма процесса передачи метаданных в «облачные» антивирусные системы для выявления компьютерных вирусов представлена на рис. 2.5.

Проведенные исследования основных подходов математического моделирования показали, что наиболее удобной, наглядной и многосторонней формой описания технологии передачи метаданных в «облачные» антивирусные системы является граф алгоритмов на основе GERT-сети.

Для рассматриваемого в статье примера под графом алгоритмов понимается орграф $G=(X,U)$ вершины $x_i$ которого отображают частные реализации $i$-х алгоритмов системы. Вершинам графа приписывается вес, соответствующий времени реализации алгоритма. (В отдельных случаях это может быть вероятность показания на тот или иной выход узлов графа, требующаяся для выполнения память, ошибки определения тех или иных величин, связанных с реализацией алгоритма и т.д.). Частные реализации

алгоритмов в рассматриваемом графе GERT-сети отождествляется дугами графа с определенными условными вероятностями и производящими функциями моментов ветви.

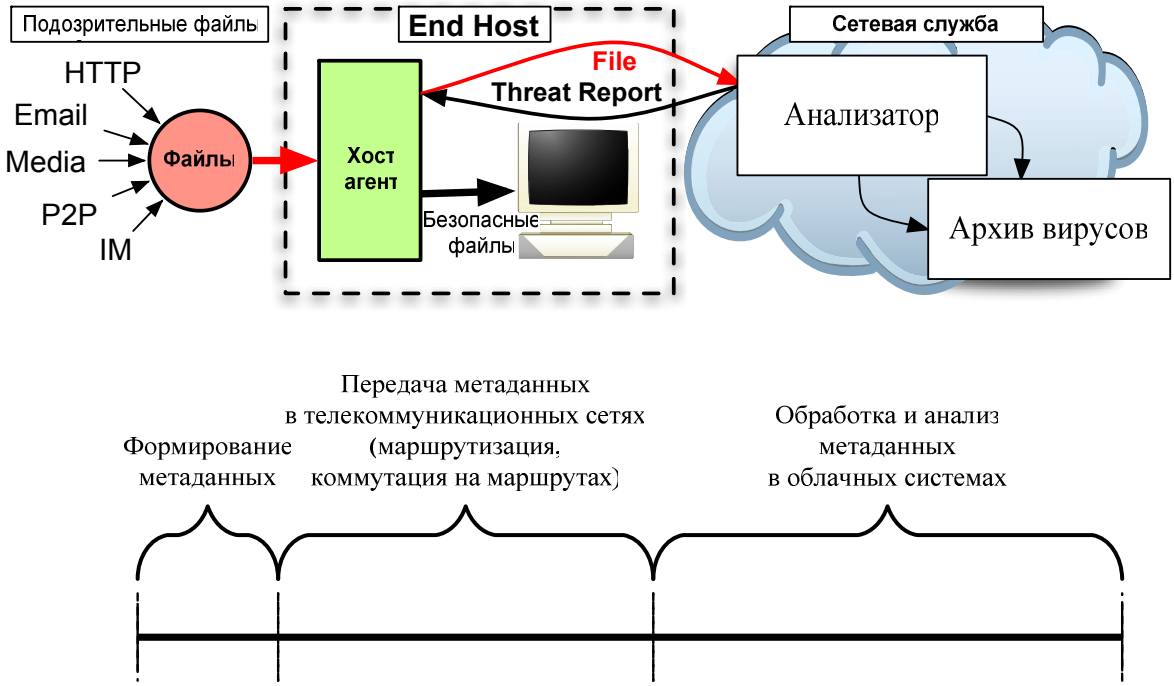



Рис. 2.5. Обобщенная структура и временная диаграмма процесса передачи метаданных в «облачные» антивирусные системы

Воспользуемся представленными на рис. 2.5 данными для разработки GERT-модели ТКС в процессе передачи метаданных в «облачные» антивирусные системы.

Типовая модель алгоритмов формирования и передачи метаданных в «облачные» антивирусные системы в соответствии с $(K+4)$ уровнем стратификации представлена на рис. 2.6.

Эта модель может быть описана следующим образом.

Ветвь (1,2) интерпретирует время формирования метаданных (сигнатур). Ветвь (2,3) задает время передачи кадра (пакета) метаданных от передатчика к трансляторам (маршрутизаторам).

Ветвь (3,3) отображает возможное неисправное состояние транслирующего коммутационного оборудования (маршрутизаторов) на выбранных маршрутах.

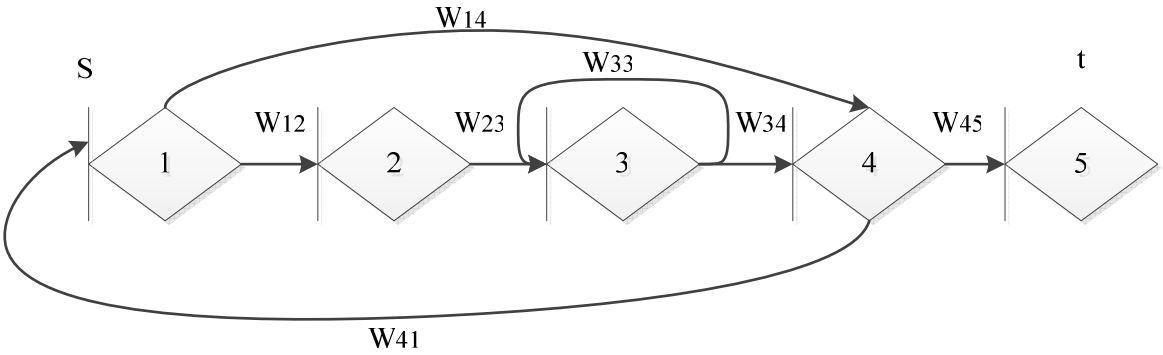



Рис. 2.6. Модель алгоритмов формирования и передачи метаданных в «облачные» антивирусные системы

Ветвь (3,4) описывает время коммутации кадра (пакета) в телекоммуникационном оборудовании.

Ветви (4,1) и (4,5) задают случайное время передачи квитанции о правильности (ошибке) доставки кадров (пакетов) в соответствии с протоколом транспортного уровня (TCP).

Узел 5 отражает состояние системы в момент анализа метаданных на предмет наличия компьютерных вирусов.

В ряде практических случаев с целью повышения вероятности выявления компьютерных вирусов существует необходимость антивирусного анализа не сформированных на оконечном оборудовании сигнатур, а данных, хранимых на этом оборудовании в полном объеме. Этой ситуации соответствует ветвь (1,4).

Ветви (3,4), (4,1) и (4,5) целесообразно описывать идентичными параметрами распределения, так как они задают схожие операции передачи данных небольшого объема.

Анализ ряда работ [16, 26, 30, 65, 72, 73, 75, 77], а также проведенные исследования процесса передачи данных в мультисервисных

телекоммуникационных сетях позволили сформировать характеристики ветвей и параметры распределения в виде, представленном в табл. 2.2.

Анализ данных, представленных в табл. 2.2. показал высокую структурную сложность разрабатываемой GERT-сети. Особенно остро данная проблема фиксируется на участке, сформированном из узлов 2-3-4 (ветви (2,3), (3,3)).

Таблица 2.2

Характеристики ветвей модели

| № п/п | Ветвь | *W*-функция | Вероятность | Производящая функция моментов |
|---|---|---|---|---|
| 1 | (1,2) | $W_{12}$ | $p_1$ | $\lambda_1 /(\lambda_1 - s)$ |
| 2 | (1,4) | $W_{14}$ | $1\text{-}p_1$ | $\lambda_2 /(\lambda_2 - s)$ |
| 3 | (2,3) | $W_{23}$ | $p_2$ | $\lambda_3 /(\lambda_3 - s)$ |
| 4 | (3,3) | $W_{33}$ | $p_3$ | $\lambda_4 /(\lambda_4 - s)$ |
| 5 | (3,4) | $W_{34}$ | $1\text{-}p3$ | $\lambda_5 /(\lambda_5 - s)$ |
| 6 | (4,5) | $W_{45}$ | $p_4$ | $\lambda_5 /(\lambda_5 - s)$ |
| 7 | (4,1) | $W_{41}$ | $1\text{-}p_4$ | $\lambda_5 /(\lambda_5 - s)$ |

С целью упрощения рассматриваемой на рис. 2.6 модели воспользуемся методикой эквивалентных упрощающих преобразований ($K$+4) уровня стратификации, описанной в подразделе 2.1.2 и работах [35, 40].

В результате упрощающих преобразований сформируем GERT-сеть, представленную на рис. 2.7. Как видно из этого рисунка в результате упрощающих преобразований ветви (2,3) и (3,3) были заменены на эквивалентную ветвь.

Обновленные данные характеристик ветвей сети представлены в табл. 2.3.

В соответствии с характеристиками ветвей GERT-сети определим эквивалентную *W*-функцию времени передачи файла как:

$$W_E(s) = \frac{W_{13}W_{34} + W_{12}W_{23}W_{34}}{1 - W_{13}W_{31} - W_{12}W_{23}W_{31}} =$$

$$= \frac{\left( \frac{p_4\lambda_5 q_1\lambda_1(\lambda_1 - s)(\lambda_3 - s)((\lambda_4 - s) - p_3\lambda_4) + p_1\lambda_1 p_4\lambda_5 p_2\lambda_3(\lambda_2 - s)}{(\lambda_2 - s)(\lambda_5 - s)(\lambda_3 - s)((\lambda_4 - s) - p_3\lambda_4)} \right)}{\left( \begin{pmatrix} (\lambda_1 - s)(\lambda_2 - s)(\lambda_5 - s)(\lambda_3 - s)((\lambda_4 - s) - p_3\lambda_4) - \\ - q_1\lambda_2 q_4\lambda_5(\lambda_1 - s)(\lambda_3 - s)((\lambda_4 - s) - p_3\lambda_4) - p_1\lambda_1 q_4\lambda_5 p_2\lambda_3(\lambda_2 - s) \end{pmatrix} \times \right.},$$
$$\left. \times (1/(\lambda_2 - s)(\lambda_1 - s)(\lambda_5 - s)(\lambda_3 - s)((\lambda_4 - s) - p_3\lambda_4)) \right)$$

где $1 - p_1 = q_1$, $1 - p_2 = q_2$, $1 - p_3 = q_3$, $1 - p_4 = q_4$.

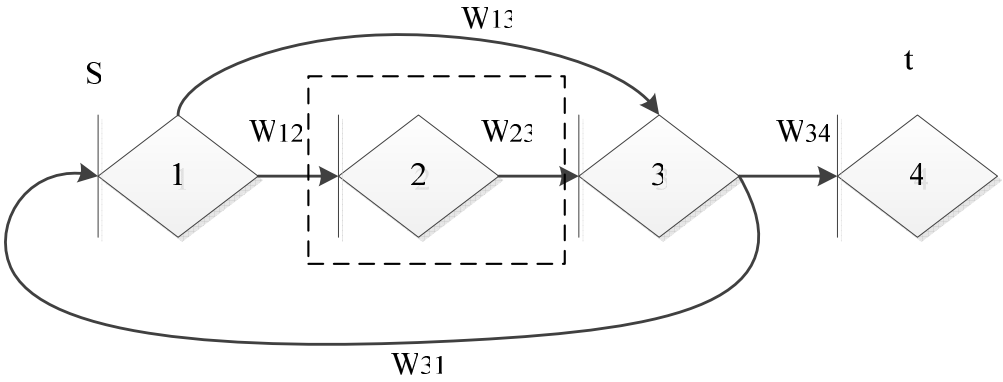



Рис. 2.7. Упрощенная модель алгоритмов формирования и передачи метаданных в «облачные» антивирусные системы

Таблица 2.3

Характеристики ветвей модели

| № п/п | Ветвь | *W*-функция | Параметр распределения |
|---|---|---|---|
| 1 | (1,2) | $W_{12}$ | $p_1\lambda_1/(\lambda_1 - s)$ |
| 2 | (1,3) | $W_{13}$ | $(1 - p_1)\lambda_2/(\lambda_2 - s)$ |
| 3 | (2,3) | $W_{23}$ | $p_2\lambda_3/(\lambda_3 - s)((\lambda_4 - s) - p_3\lambda_4)$ |
| 4 | (3,4) | $W_{34}$ | $p_4\lambda_5/(\lambda_5 - s)$ |
| 5 | (3,1) | $W_{31}$ | $(1 - p_4)\lambda_5/(\lambda_5 - s)$ |

Проведенные исследования показали, что в сложных GERT-сетях с возможными циклами отсутствуют простые методы нахождения особых

точек функции $\Phi_E(z)$ замены действительных переменных $(z=-i\varsigma)$, где $\varsigma$ – действительная переменная. Связано это с тем, что для нахождения особых точек необходимо решать нелинейные уравнения, и чем сложнее структура GERT-сети, тем сложнее и исходное уравнение [68]. Поэтому в ходе моделирования выполняя комплексное преобразование получим:

$$\Phi(z)=\frac{uz^3-kz^2+wz+h}{\left(z^3+vz^2+rz+c\right)}, \tag{2.3}$$

где:

$$u=p_4\lambda_5 q_1\lambda_2,$$

$$k=p_4\lambda_4 q_1\lambda_2\left(p_3\lambda_4-\lambda_3-\lambda_1-\lambda_4\right),$$

$$w=p_4\lambda_5 q_1\lambda_2\cdot\left(p_3\lambda_3\lambda_4-\lambda_1\lambda_3-\lambda_3\lambda_4-\lambda_1\lambda_4+p_3\lambda_1\lambda_4\right),$$

$$h=p_4\lambda_4 q_1\lambda_1\lambda_2\lambda_3\lambda_4 q_3,$$

$$v=\lambda_3-\lambda_4-\lambda_2+q_1q_4\lambda_2\lambda_5+p_3\lambda_4,$$

$$r=\lambda_3\lambda_4+\lambda_3\lambda_2-q_1\lambda_2q_4\lambda_5\lambda_3-p_3\lambda_3\lambda_4+\lambda_2\lambda_4-$$
$$-q_1\lambda_2q_4\lambda_5\lambda_4-p_3\lambda_2\lambda_4+q_1\lambda_2q_4\lambda_5p_3\lambda_4,$$

$$c=\lambda_3\lambda_4\lambda_2-q_1\lambda_2q_4\lambda_3\lambda_4\lambda_5-p_3\lambda_3\lambda_4\lambda_2+q_1\lambda_2q_4\lambda_3\lambda_4p_3.$$

Из выражения (2.3) видно, что функция $\Phi(z)$ имеет только простые полюсы определяемые корнями уравнения $z^3+vz^2+rz+c=0$. В этом случае плотность распределения вероятностей времени передачи сообщения равна:

$$\varphi(x)=\frac{1}{2\pi i}\int_{-i\infty}^{i\infty}e^{zx}\frac{uz^3-kz^2+wz+h}{\left(z^3+vz^2+rz+c\right)}dz. \tag{2.4}$$

Используя специализированный математический пакет *Mathcad*, определим простые полюсы $z$ функции $\Phi(z)$ и найдем плотность распределения вероятностей $\varphi(x)$ времени передачи метаданных в

«облачные» антивирусные системы. При этом в качестве начальных данных определим следующие параметры ветвей GERT-сети:

$$p_1 = 0{,}9\,,\ p_2 = 0{,}99999\,,\ p_3 = 0{,}99999\,,\ p_4 = 0{,}99999\,,$$

$$\lambda_1 = 1\,,\ \lambda_2 = 0{,}099\,,\ \lambda_3 = 0{,}9\,,\ \lambda_4 = 0{,}5\,,\ \lambda_5 = 0{,}4\,.$$

Для указанного примера функция $\Phi(z)$ имеет простые полюса:

$$z := \begin{pmatrix} -0.67 \\ 0 \\ -0.117 \end{pmatrix}.$$

В соответствии с формулой (2.4) $\varphi(x)$ равна:

$$\begin{aligned}
&\frac{1}{z} 0{,}159155 \times 2{,}71828^{(-0{,}0835025 - 0{,}364433i)z} \times \\
&\times (z 2{,}71828^{(0/920508 + 0{,}364433i)z}\, Ei((x - 0{,}837005)z) \times \\
&\times (1/02026h - 0{,}714769k + 0{,}85396\nu + 0{,}598265) + \\
&+ 2{,}71828^{(0{,}728866i)z}\, zEi((x + (0{,}0835025 - 0{,}364433i))z) \times \\
&\times (-(0{,}142616 - 0{,}131097i)k - (0{,}42698 + 0{,}293502i)\nu + \\
&+ (0{,}0358675 + 0{,}0629208i) + (-0{,}510128 + 1{,}28851i)h) - \\
&- (0{,}510128 + 1{,}28851i)hzEi((x + (0{,}0835025 + 0{,}364433i))z) - \\
&- (0{,}142616 + 0{,}131097i)kzEi((x + (0{,}0835025 + 0{,}364433i))z) - \\
&- (0{,}42698 - 0{,}293502i)\nu zEi((x + (0{,}0835025 + 0{,}364433i))z) + \\
&+ (0{,}0358675 + 0{,}0629208i)zEi((x + (0{,}0835025 + 0{,}364433i))z) + \\
&+ 2{,}71828^{z(x + (0{,}0835025 + 0{,}364433i))}) + const
\end{aligned}$$

На рис. 2.8. представлен график плотности распределения времени передачи метаданных.

Как видно из этого рисунка максимальные значения плотности распределения времени формирования и передачи приходится на промежуток от 1 до 3 с.

Таким образом, на основе GERT-сети разработана математическая модель технологии передачи метаданных в «облачные» антивирусные системы, которая отличается от известных учетом показателей реальной

надежности и особенностей многопутевой маршрутизации в соответствии с протоколами сетевого уровня.

Модель может быть использована для исследования процессов и технологий распространения и лечения ЗПО в информационно-телекоммуникационных системах, а также локальных компьютерных сетях, при разработке новых протоколов, алгоритмов и программ управления сетевыми и канальными ресурсами ТКС, проектировании новых средств антивирусной защиты данных.

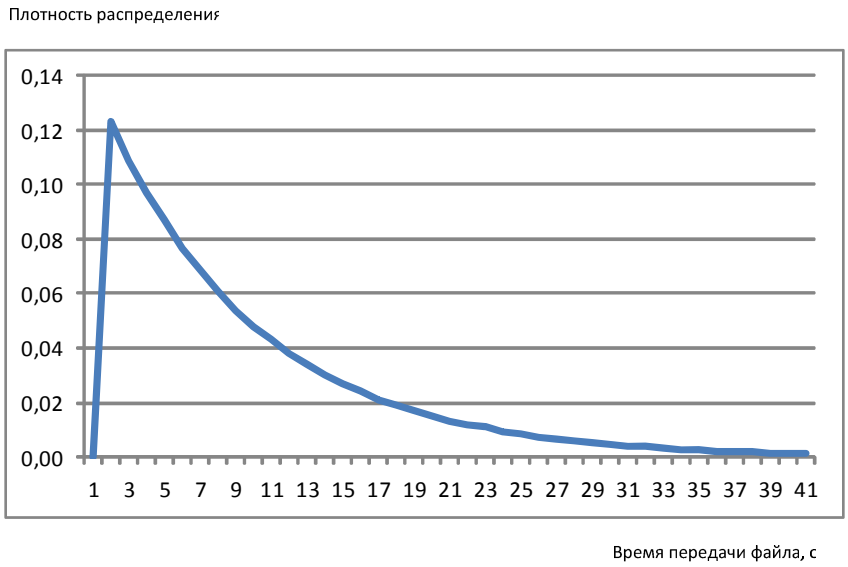



Рис. 2.8. Плотность распределения времени передачи метаданных в «облачные» антивирусные системы

Применение GERT-сетей в ходе математического моделирования даст возможность использования результатов, полученных в аналитическом виде (функции, плотности распределения) для проведения сравнительного анализа и исследований, более сложных информационно-телекоммуникационных систем математическими методами.

## 2.3. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях

Проведем сравнительные исследования разработанной математической модели технологии распространения компьютерных вирусов в ТКС. Для такого исследования и соответственно оценки в качестве эталонной выберем математическую модель *PSIDDR*, представленную в работах [63, 64, 68] на основе биологического подхода моделирования. По данным источников [63, 64] указанная математическая модель наиболее адекватно описывает процесс распространения компьютерных вирусов и учитывает пять возможных состояний узлов ТКС в процессе их функционирования в условиях внешних деструктивных воздействий.

Исходя из выделенных в [63, 64] данных, в математической модели *PSIDDR*, обобщенная структура ТКС может быть представлена с помощью выражения:

$$N = S(t) + I(t) + D(t) + R(t) + X(t),$$

где:

$S(t)$ – количество уязвимых объектов;

$I(t)$ – количество зараженных объектов;

$R(t)$ – количество вылеченных объектов, обладающих иммунитетом;

$D(t)$ – количество объектов, в которых обнаружен вирус;

$X(t)$ – количество выведенных из строя узлов;

$N$ – общее количество объектов в системе.

С учетом указанных особенностей функционирования ТКС модель *PSIDDR* математически можно представить в виде системы:

$$\begin{cases} \dfrac{dS(t)}{dt} = -\beta \dfrac{S(t)I(t)}{N} - \alpha S(t) \\ \dfrac{dI(t)}{dt} = \beta \dfrac{S(t)I(t)}{N} - (\gamma + \chi)I(t) \\ \dfrac{dR(t)}{dt} = \omega D(t) + \alpha S(t) \\ \dfrac{dD(t)}{dt} = \gamma I(t) - (\omega + \chi)D(t) \\ \dfrac{dX(t)}{dt} = \chi I(t) + \chi D(t) \\ \dfrac{dS(t)}{dt} + \dfrac{dI(t)}{dt} + \dfrac{dR(t)}{dt} + \dfrac{dD(t)}{dt} + \dfrac{dX(t)}{dt} = 0, \end{cases} \quad (2.5)$$

где:

$\beta$ – частота заражения;

$\alpha$ – вероятность иммунизации до стадии заражения;

$\chi$ – вероятность того, что вирус атакует узел с фатальными последствиями;

$\gamma$ – вероятность того, что вирус на данном узле будет выявлен;

$\omega$ – вероятность лечения;

$S(t)$ – количество уязвимых объектов;

$I(t)$ – количество зараженных объектов;

$R(t)$ – количество вылеченных (с иммунитетом) объектов;

$X(t)$ – количество выведенных из строя объектов;

$D(t)$ – количество обнаруженных зараженных объектов (на первой стадии равно 0);

$N$ – общее количество объектов в системе.

В качестве исходных параметров моделирования и сравнительной оценки были выбраны числовые значения характеристик процесса распространения компьютерных вирусов, характерные реальному функционированию ТКС локального уровня:

– $\alpha$= 0,08;

– $\gamma$= 0,3;

– ω= 0,3;

– β= 0,2.

На рис. 2.9 представлены графики зависимости количества зараженных (*I*), выведенных из строя (*X*), и вылеченных (*R*) объектов от времени функционирования компьютерной системы, в различных начальных условиях зараженности сети.

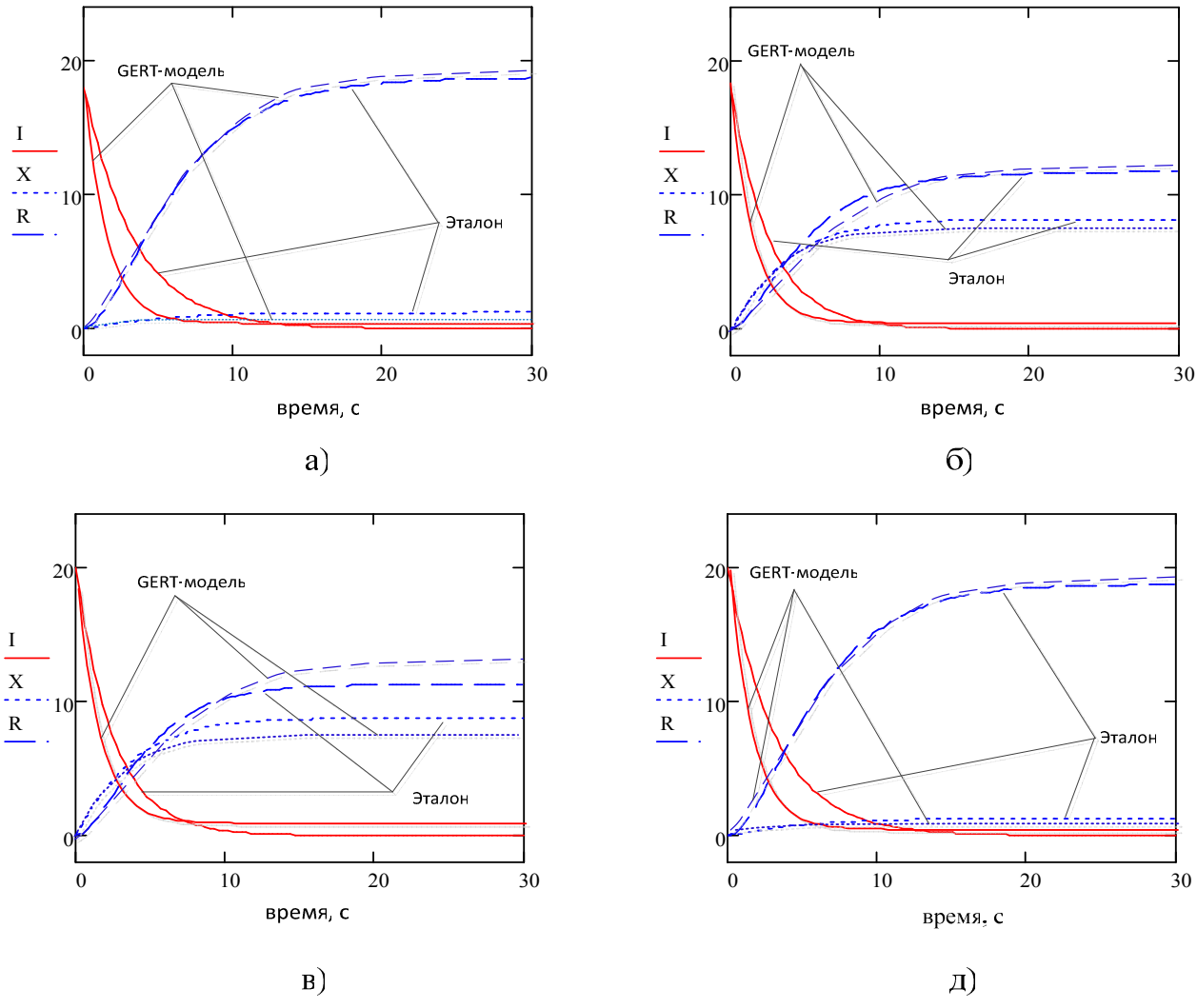



Рис. 2.9. Графики зависимости количества зараженных (*I*), выведенных из строя (*X*), и вылеченных (обладающих иммунитетом (*R*)) объектов от времени функционирования информационно-телекоммуникационной сети

Так, на рис. 2.9.а приводится семейство кривых, характеризующее перечисленные процессы в условиях, когда вероятность $\chi = 0{,}01$, а уровень заражения ТКС на момент начала второй стадии $U = \frac{I}{N} = 0{,}9$. Аналогично на рис. 2.9.б определены следующие начальные условия: $\chi = 0{,}1$, $U=0{,}9$; на рис. 2.9.в: $\chi = 0{,}1$, $U=1$, на рис. 2.9.д: $\chi = 0{,}01$, $U = 1$.

Как видно из рисунка, в первом исследуемом случае (рис. 2.9.а), конечное количество выведенных из строя объектов $X \approx \{1,2\}$, во втором случае (рис. 2.9.б) это количество $X \approx \{7,8\}$, в третьем (рис. 2.8.в) – $X \approx \{8,9\}$, в четвертом (рис. 2.9.д) – $X \approx \{1,2\}$.

Кроме этого из рис. 2.9. видно, что учет в GERT-модели ключевой информации о состояниях телекоммуникационных узлов (интеллектуальных узлов коммутации) в процессе деструктивных воздействий компьютерных вирусов позволил повысить точность полученных результатов по сравнению с эталоном до 1,4 раза.

## Выводы по разделу 2

В разделе разработан метод априорной оценки требований оперативности передачи данных в условиях воздействия компьютерных вирусов, в основу которого положены математическая модель технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях и математическая GERT-модель технологии передачи метаданных в «облачные» антивирусные системы.

Основными результатами второго раздела являются:

Получила дальнейшее развитие математическая модель технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях, в отличие от известных, учитывающая ключевую информацию о состояниях телекоммуникационных узлов в процессе деструктивных воздействий компьютерных вирусов, а также

фактор использования «облачного» антивирусного обеспечения в процессе лечения, что позволило повысить точность полученных результатов по сравнению с известными до 1,4 раза.

Разработана структурно-логическая GERT-модель технологии распространения компьютерных вирусов. Это позволило определить эквивалентную *W*-функцию времени распространения в ТКС наиболее опасных компьютерных вирусов типа *Flame* с конечными результатами лечения и иммунизации узлов ТКС, а также учесть фактор выхода из строя телекоммуникационных узлов.

Представлена методика эквивалентных упрощающих преобразований GERT-модели технологии распространения компьютерных вирусов с возможностью декомпозиции исследуемого объекта на отдельные страты.

Представлены примеры возможной стратификации процесса функционирования информационно-телекоммуникационной сети с учетом фактора деструктивного воздействия компьютерных вирусов на систему.

В ходе математического моделирования технологии функционирования информационно-телекоммуникационной сети был учтен фактор использования «облачного» антивирусного обеспечения в процессе лечения узлов ТКС.

Разработана математическая GERT-модель технологии передачи метаданных в «облачные» антивирусные системы, которая отличается от известных учетом показателей реальной надежности и особенностей многопутевой маршрутизации в соответствии с протоколами ($K$+4) уровня стратификации.

Основные научные результаты, изложенные во втором разделе, опубликованы в работах автора [32, 35, 36, 46, 47, 52].

# РАЗДЕЛ 3
# РАЗРАБОТКА МЕТОДА УПРАВЛЕНИЯ ДОСТУПОМ В ИНТЕЛЛЕКТУАЛЬНЫХ УЗЛАХ КОММУТАЦИИ

В данном разделе разработан метод управления доступом в интеллектуальных узлах коммутации, включающий в себя математическую модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета и усовершенствованный алгоритм управления доступом к облачным телекоммуникационным ресурсам.

На основе модели многоканальной СМО $\overline{M}_r/M/V_r/K_r$ а также разработанной GERT-модели интеллектуального узла коммутации проведены исследования и анализ показателей качества функционирования ТКС. Определены эквивалентная *W*-функция, функция распределения и плотность распределения времени обслуживания информационных пакетов метаданных в интеллектуальных узлах коммутации при их передаче в облачные антивирусные системы

Определено, что в качестве дополнительного критерия присвоения информационному пакету «эталонного» приоритета могут выступать соответствующие им значения показателя вероятности $P_{присв}$ присвоения приоритета.

## 3.1. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета

В современных условиях динамичного развития различных подходов анализа и синтеза телекоммуникационных сетей, интегрирующихся в единую информационно-телекоммуникационную технологию [55, 58] актуальными становятся вопросы разработки и применения общих методов обеспечения

качества обслуживания на основе выделения отдельных классов качества и реализации для них унитарных алгоритмов управления, таких как приоритезация информационных пакетов, резервирование телекоммуникационных ресурсов, организация очередей в узлах коммутации и др. На рис. 3.1. представлена классификация механизмов управления качеством обслуживания на основе рекомендаций международного союза электросвязи МСЭ-Т *Y.1291* [54].

Появление новых дестабилизирующих факторов связанных с воздействием злоумышленного программного обеспечения на процесс функционирования информационно-телекоммуникационных сетей заставляет пересмотреть общие возможности существующих механизмов управления качеством обслуживания и разработать ряд конкретных предложений (алгоритмов) их адаптации к возможным неправомерным действиям участников телекоммуникационного обмена.

Таким образом, возникает необходимость развития сетевых и телекоммуникационных технологий и разработки адекватных, указанным на рис. 3.1. механизмам, методов управления сетевыми ресурсами, которые могли бы обеспечить:

– качество обслуживания и информационную безопасность при совместной передаче разнородного трафика с учетом условий ограничения сетевых ресурсов, реальной надежности телекоммуникационного оборудования и возможного внешнего воздействия злоумышленного или иного характера;

– безопасность функционирования отдельных узлов информационно-телекоммуникационных систем в условиях воздействий злоумышленного программного обеспечения;

– устойчивость (надёжность, живучесть, функциональную безопасность) функционирования в указанных выше условиях и др.

Как было указано во втором разделе, одним из механизмов эффективного противодействия злоумышленному программному обеспечению является использование «облачных» антивирусных ресурсов.


Рис. 3.1. Классификация механизмов управления качеством обслуживания

Исследования основных процедур обмена данными в информационно-телекоммуникационных системах показали, что одну из ключевых ролей при обеспечении своевременности доставки метаданных (сигнатур) в «облачные» антивирусные системы играют механизмы управления передачей. При этом их основные алгоритмы реализованы непосредственно в узлах коммутации. Данный факт позволил сделать вывод о необходимости разработки метода

управления сетевыми ресурсами с учетом усовершенствованных процедур организации и планирования очередей.

### 3.1.1. Общая постановка задачи описания процессов функционирования узла коммутации

В соответствии данными, указанными в [72-77], структурно-функциональное построение ТКС нового поколения (*NGN*-сетей) неоднородно. Данный фактор особенно ярко выражен на начальных этапах построения ТКС.

Следует заметить, что при объединении только низкоскоростного трафика, создаются предпосылки для использования моделей простейших потоков [23, 24]. Это обусловлено тем, что взаимное наложение большого числа малых независимых ординарных стационарных (нестационарных) потоков с различным последействием (теорема Хинчина) [24], а также преобразование потоков в сети (суммирование, просеивание) [1, 4, 7] в пределе даёт поток близкий к простейшему:

$$a_r = a_r(t) = 1 - e^{(-\lambda_r \cdot t)}, \quad \lambda_r \geq 0, t \geq 0, \tag{3.1}$$

где:

$\lambda_r$ – параметр потока, приведённый к параметрам передачи с помощью выражения:

$$\lambda_r = \lambda_c(r) \cdot q(r) \cdot \eta_r,$$

$\lambda_c(r)$ – интенсивности поступления сообщений;

$q(r) = \left(\mu_c(r) \cdot t_{\text{сегм}}(r)\right)^{-1}$ – среднее число пакетов в сообщении $r$-го приоритета;

$t_{\text{сегм}}(r) = \dfrac{L(r)}{\nu_{\text{прд}}(r)}$ – среднее время сегментации пакетов $r$-го приоритета;

$L(r)$ – длина информационной части пакета $r$-го приоритета;

$\nu_{\text{прд}}(r)$ – скорость передачи (обработки) информации $r$-го приоритета;

$\eta_r = \dfrac{L_{\text{пак}}(r)}{L(r)}$ – накладные расходы на пакетное преобразование;

$L_{\text{пак}}(r)$ – длина пакета $r$-го приоритета.

При поступлении в ТКС пакеты различных классов приоритетности разбиваются на пакеты различной длины $L(r)$, при ограничении их максимального размера. Данное предположение позволяет сделать вывод о возможности использования при проектировании таких сетей, в соответствующих расчетах, показательного закона распределения случайной величины длительности их обслуживания в узлах коммутации [9, 55, 70]. В этом случае длительность обслуживания пакетов приоритетов $r = \overline{1,R}$ случайная величина с функцией распределения [55]:

$$B(t) = 1 - e^{\left(-t/b\right)},\ t \geq 0, b \geq 0, \tag{3.2}$$

и конечными первыми двумя моментами:

$$b = \int_0^\infty t dB(t) = \frac{1}{\mu_{ср}}, \tag{3.3}$$

$$b^{(2)} = \int_0^\infty t^2 dB(t) = \frac{2}{\mu_{ср}^2}, \tag{3.4}$$

$$\mu = \sum_{r=1}^{R} \frac{\lambda_r}{\Lambda_r} \times \frac{\nu_{\text{прд}}(r)}{L_{\text{пак}}(r)}, \tag{3.5}$$

где $\mu_{ср}$ – средняя интенсивность обслуживания пакетов.

В описанном выше примере в узле коммутации реализуется следующая дисциплина обслуживания.

а) Если в момент поступления пакета с любым приоритетом $r = \overline{1,R}$ имеются свободные каналы (состояние узла коммутации $0 \leq i \leq V-1$), то он немедленно поступает на обслуживание.

б) В случае занятости всех каналов (состояние узла коммутации $V \le i \le V + K$) поступивший пакет $\ell$-го приоритета становится в очередь и принимается на обслуживание раньше пакета $j$-го приоритета, если $\ell < j$. Если в момент поступления пакета $\ell$-го приоритета в очереди имелось $K$-пакетов (буфер заполнен полностью), то поступивший пакет:

– принимается в очередь при условии, что в ней имеются пакеты с более низким $j$-м приоритетом, при этом последний пакет с низшим приоритетом вытесняется из системы и, в последующем, не оказывает на неё никакого влияния;

– теряется при условии, что в очереди имеются только пакеты с более высоким и/или равным приоритетом.

в) Для пакетов $r$-го (одинакового) приоритета, находящихся в очереди, реализуется система обслуживания *FIFO*.

В представленной дисциплине обслуживания в узле коммутации, при постановке пакетов в очередь и управлении очередью, действуют абсолютные, а при обслуживании – относительные приоритеты. Применение абсолютных приоритетов только для управления очередью обеспечивает обслуживание пакетов без прерываний, но при этом минимизируются потери и среднее время ожидания приоритетных пакетов.

В то же время описанная выше дисциплина обслуживания имеет и ряд недостатков, связанных в первую очередь с отсутствием учета факторов злоумышленных или иных внешних воздействий на ТКС.

Поэтому в условиях деструктивных внешних воздействий, а также частого выхода из строя телекоммуникационного оборудования использование данной модели при проектировании ТКС негативно влияет на процесс обеспечения таких показателей качества обслуживания как информационная и функциональная безопасность, надежность.

Проведенные исследования показали, что для устранения указанных недостатков целесообразно использовать математическую модель узла

коммутации типа $\overrightarrow{M_r}/M/V_r/K_r$ с относительными приоритетами, резервированием ресурсов и учётом реальной надёжности обслуживающих приборов.

### 3.1.2. Модель узла коммутации с относительными приоритетами, резервированием ресурсов и учётом реальной надёжности обслуживающих приборов

При допущениях, приведенных в подразделе 3.1.1. (относительно: аппроксимации входящих потоков пакетов классов $r=\overline{1,R}$ данными с характеристиками пуассоновского закона распределения; обслуживания с относительными приоритетами $r=\overline{1,R}$ по классам качества услуг, с учетом категорий пользователей и подсистем; наличия $V$ обслуживающих приборов, имеющих конечную надёжность; переменной длины пакетов, характеризуемой показательной функцией распределения (3.2) с параметром $\mu$, определяемым выражением (3.5)), с целью эффективного управления трафиком и обеспечения заданных показателей качества обслуживания (в том числе информационной и функциональной безопасности), в условиях ограниченных ресурсов ТКС и возможных злоумышленных или иных воздействий, может применяться дисциплина обслуживания с относительными приоритетами $r=\overline{1,R}$, неполнодоступным включением каналов $V_r$, и совместным (раздельным) использованием накопителей $K_r$. Это позволит обеспечить резервирование коммуникационных ресурсов для высокоприоритетного трафика (в первую очередь метаданных в «облачные» антивирусные системы) [113, 114].

Проведенный анализ основных алгоритмов управления очередями в коммуникационном оборудовании ТКС показал, что в настоящее время существует несколько видов дисциплин (способов) обслуживания очередей, реализующих резервирование ресурсов (разделение процессора):

– справедливая организация очередей (*Fair Queuing, FQ*);

– очереди приоритетов (*Priority Queuing, PQ*);

– организация произвольных настраиваемых очередей (*Custom Queuing, CQ*);

– взвешенная справедливая организация очередей (*Weighted Fair Queuing, WFQ*);

– обслуживание очередей на основе классов (*Class Based Weighted Fair Queuing, CBWFQ*) и др. [5, 28].

Сравнительные исследования указанных алгоритмов показали, что наиболее эффективными, с точки зрения обеспечения качества обслуживания, являются алгоритмы *WFQ* и *CBWFQ*, являющиеся производными алгоритмов *CQ*. Поэтому дальнейшие исследования в большей степени будут основаны на положениях обслуживания очередей и управления *WFQ* и *CBWFQ*.

Представим телекоммуникационную систему, в которой предоставляемые услуги разбиты на несколько классов качества обслуживания (*QoS*), имеющих соответствующие приоритеты по задержке и потерям пакетов (например, передача информационно-измерительных данных мониторинга, телефония, передача почтовой информации, видеоконференцсвязь и др.). При этом общее число приоритетов для видов услуг, категорий пользователей и подсистем составляет $R$.

Предположим, что на вход интеллектуального узла коммутации поступают простейшие потоки пакетов $r$-ых приоритетных классов $\{a_1,\ldots,a_r,\ldots,a_R\}$, которые занумерованы в порядке убывания их приоритета. Каждый приоритетный класс характеризуется интенсивностью поступления пакетов $\lambda_r$: $\lambda_r > 0$.

Пусть в частном случае приоритеты объединены в три группы $r_1 = 1$, $r_2 = \overline{2,J}$, $r_3 = \overline{J+1,R}$ соответствующие обслуживанию:

– $r_1 = 1$ – трафика метаданных для передачи в «облачные» антивирусные системы;

– $r_2 = \overline{2, J}$ – трафика реального времени, критичного к сетевым задержкам (телефония, видеоконференцсвязь, данные объективного контроля, и т.д.);

– $r_3 = \overline{J+1, R}$ – трафика данных, критичного к потерям и не критичного к сетевым задержкам, включая потоковый трафик (аудио-, видео по требованию и др.) и эластичный трафик (электронная почта, web-приложения и др.).

При этом самым высоким приоритетом пользуются метаданные для передачи в «облачные» антивирусные системы.

В соответствии с этим в узлы коммутации информационно-телекоммуникационных систем, представляемые различными интеллектуальными устройствами (шлюзами, контроллерами шлюзов, коммутаторами, маршрутизаторами и др.) транспортной сети, от пользователей различных категорий и подсистем поступают потоки сообщений различных классов. Интенсивности поступления и обслуживания сообщений характеризуются параметрами $\lambda_c(r)$ и $\mu_c(r)$, $r = \overline{1, R}$ соответственно, скорость поступления (передачи) сообщений $v_{\text{прд}}(r)$. При этом поступающие в узлы коммутации сообщения преобразуются в пакетную форму и образуют $R$ независимых потоков пакетов $\{a_1, \ldots, a_r, \ldots, a_R\}$ с интенсивностями $\{\lambda_1, \ldots, \lambda_r, \ldots, \lambda_R\}$.

Исследуемый интеллектуальный узел коммутации ТКС (рис. 3.2) состоит из $0 < V < \infty$ обслуживающих устройств, имеющих идентичные тактико-технические характеристики, определяющиеся возможностями производителей телекоммуникационного оборудования, и буфера памяти объёма $0 < K < \infty$.

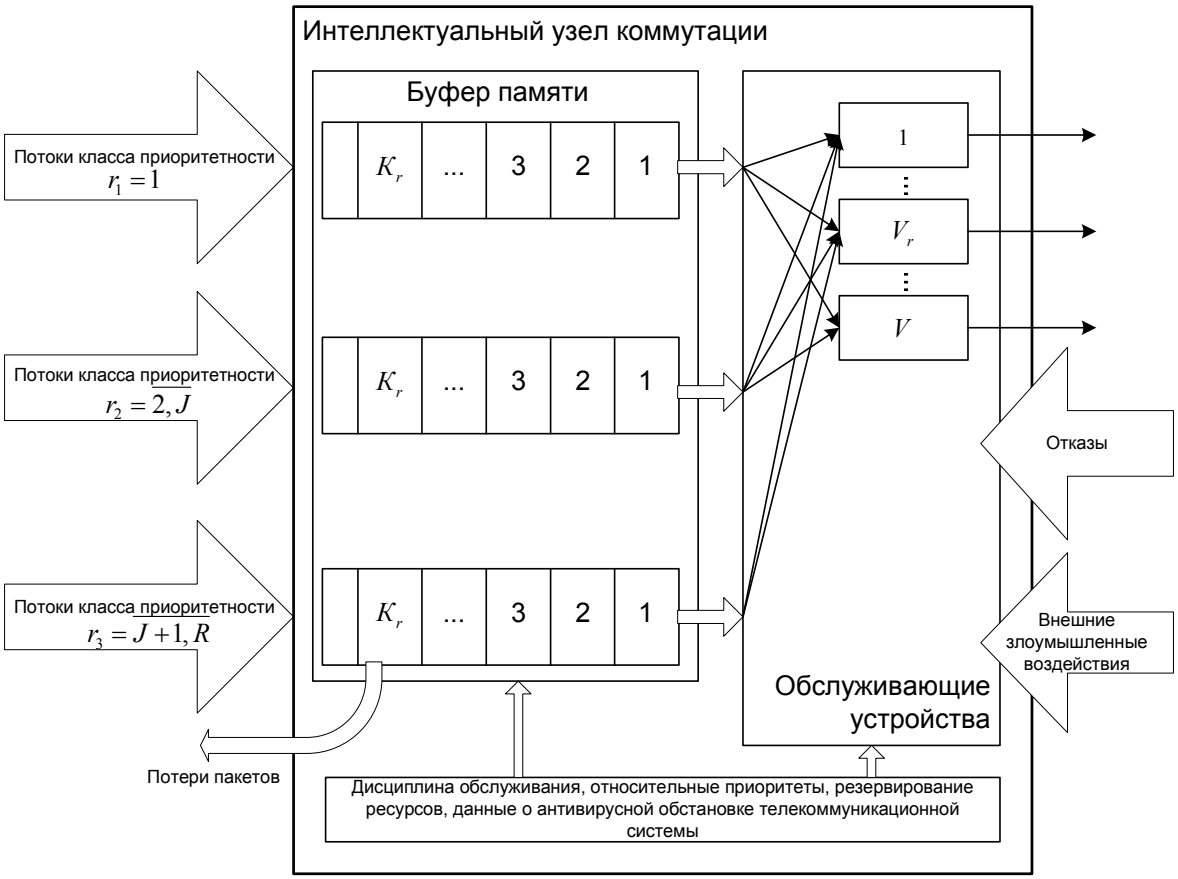



Рис. 3.2. Структура исследуемой модели интеллектуального узла коммутации ТКС с относительными приоритетами и резервированием ресурсов

В узле коммутации вводятся ограничения на ресурсы обслуживающих устройств $V_r \le V$ и размер буфера памяти $K_r \le K$ пакетами различных приоритетных классов. При этом для пакетов с приоритетом $r_1$ доступны все $V$ обслуживающих устройств $V_r = V$ и выделена часть буфера $K_r \le K$ из общего объёма буфера $K$, определяемая в соответствии с усовершенствованным алгоритмом управления доступом к «облачным» телекоммуникационным ресурсам, описанным ниже в подразделе 3.2.

Для пакетов приоритетов $r_2 = \overline{2, J}$ доступна часть $V_r \le V$ обслуживающих устройств, неиспользуемая в данный момент времени пакетами метаданных приоритета $r_1$, и определяемая усовершенствованным алгоритмом управления доступом к «облачным» телекоммуникационным

ресурсам, а также выделена часть буфера $K_r \le K$ из общего объёма буфера $K$.

Для пакетов оставшихся приоритетов $r_3 = \overline{J+1, R}$ вводится ограничительный порог – доступна только часть общих обслуживающих устройств $V_r < V$ и выделена часть буфера $K_r < K$ из общего объёма буфера $K$, так что $\sum_{r=1}^{R} K_r = K$. Внутри каждого из приоритетных классов $r_1$, $r_2 = \overline{2, J}$, $r_3 = \overline{J+1, R}$ выделенный буфер используется совместно пакетами данных приоритетных классов.

Следует заметить, что при такой организации распределения ресурсов узлов коммутации вероятность потери $P_{r_1}$ в буфере памяти информационных пакетов приоритета класса $r_1$ практически нулевая ($P_{r_1} = 0$). Аналогичная вероятность $P_{r_2}$ потери информационных пакетов приоритета класса $r_2$ $P_{r_2} \approx 0$.

В исследуемом интеллектуальном узле коммутации ТКС обслуживание пакетов происходит в соответствии со следующей дисциплиной:

1. Если в момент поступления информационного пакета с приоритетом $r_1$, $r_2 = \overline{2, J}$, $r_3 = \overline{J+1, R}$ имеются свободные из доступных для данного приоритетного класса обслуживающих устройств, то он в соответствии с алгоритмом управления доступом к «облачным» телекоммуникационным ресурсам поступает на обслуживание.

2. В случае занятости всех доступных обслуживающих устройств (состояние интеллектуального узла коммутации $V_r \le i \le V_r + K_r$) организуются раздельные очереди для пакетов с приоритетами $r_1$, $r_2 = \overline{2, J}$ и $r_3 = \overline{J+1, R}$ соответственно. При этом в каждой из них реализуется следующая дисциплина обслуживания: при постановке пакетов в очередь действуют абсолютные приоритеты, а при выборке пакетов на обслуживание – относительные приоритеты в соответствии с

усовершенствованным алгоритмом управления доступом к «облачным» телекоммуникационным ресурсам (см. подраздел 3.2).

Применение абсолютных приоритетов при постановке в очередь уменьшает среднее время ожидания приоритетных пакетов из групп $r_1$ и $r_2 = \overline{2, J}$, что позволяет в конечном итоге повысить информационную безопасность ТКС (улучшить антивирусную защиту) и обеспечить заданные показатели качества (*QoS*) обслуживания данных.

В результате в каждой очереди пакет $\ell$-го приоритета принимается на обслуживание раньше пакета $j$-го приоритета, если $\ell < j$. Кроме того, если в момент поступления пакета $\ell$-го приоритета в очередях $r_1$, $r_2 = \overline{2, J}$ или $r_3 = \overline{J+1, R}$ имелось $K_r$ пакетов, то поступивший пакет обрабатывается следующим образом:

– или принимается в очередь при условии, что в ней имеются пакеты с более низким $j$-м приоритетом, при этом последний пакет с низшим приоритетом вытесняется из узла коммутации и в последующем не оказывает на него никакого влияния;

– или теряется при условии, что в очереди имеются только пакеты с более высоким и/или равным $j$-м приоритетом.

3. Пакеты $r$-го приоритета, находящиеся в очереди $r_1$, $r_2 = \overline{2, J}$ или $r_3 = \overline{J+1, R}$, обслуживаются в соответствии с усовершенствованным алгоритмом управления доступом к «облачным» телекоммуникационным ресурсам.

В целом представленная дисциплина обслуживания информационных пакетов в интеллектуальном узле коммутации реализует резервирование сетевых ресурсов на основе стратегии подвижной границы.

Проведем исследования и анализ показателей качества функционирования интеллектуальных узлов коммутации. Для этого используем модель многоканальной СМО $\overline{M}_r / M / V_r / K_r$.

### 3.1.3. Исследования показателей качества функционирования интеллектуальных узлов коммутации

Для исследования показателей качества функционирования интеллектуальных узлов коммутации типа $\overline{M}_r/M/V_r/K_r$ воспользуемся методикой структурно-логического GERT-моделирования, описанной в разделе 2. Рассмотрим её отличительные особенности.

В соответствии с моделью технологии функционирования интеллектуального узла коммутации ТКС с относительными приоритетами и резервированием ресурсов (см. подраздел 3.1.1.) изменение состояний данного узла представим GERT-сетью (рис. 3.3). Каждая ветвь $r_1$, $r_2 = \overline{2, J}$, $r_3 = \overline{J+1, R}$ данной сети условно описывает отдельную многопотоковую систему обслуживания с выделенными $(V_r, K_r)$ и совместно используемыми $(V_R)$ ресурсами.

Эта модель может быть описана следующим образом.

Узел 1 отражает состояние системы в первоначальный момент получения информационных пакетов любого из возможных классов приоритетов $r_1$, $r_2 = \overline{2, J}$, $r_3 = \overline{J+1, R}$.

Узел 2 фиксирует состояние системы, при которой поступившие информационные пакеты обрабатываются в соответствии с алгоритмом управления доступом к «облачным» телекоммуникационным ресурсам в режиме совместно используемых $(V_R)$ ресурсов.

Узел 3 интерпретирует состояние системы в момент, когда на интеллектуальный узел коммутации поступает пакет $r_1$ класса приоритетности, и при этом в соответствии с алгоритмом управления доступом к «облачным» телекоммуникационным ресурсам существует необходимость фиксации и выделения отдельных вычислительных ресурсов.

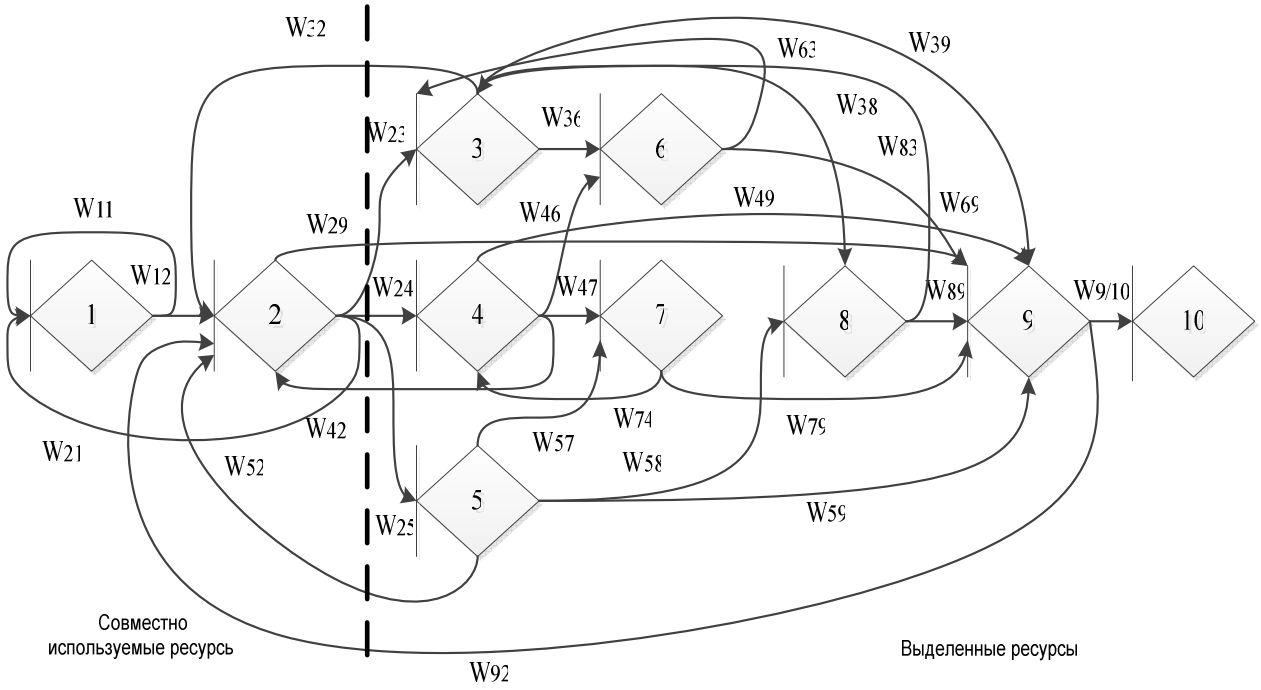



Рис. 3.3. Структурно-логическая *GERT*-модель технологии функционирования интеллектуального узла коммутации ТКС с относительными приоритетами и резервированием ресурсов

Узлы 4 и 5 описывают состояние системы в момент, когда на интеллектуальный узел коммутации поступают пакеты $r_2 = \overline{2, J}$ и $r_3 = \overline{J+1, R}$ класса приоритетности соответственно и, аналогично узлу 3, существует необходимость фиксации и выделения отдельных вычислительных ресурсов.

Узел 6 отражает состояние исследуемого объекта, когда в интеллектуальном узле коммутации обрабатываются одновременно информационные пакеты $r_1$ и $r_2 = \overline{2, J}$ классов приоритетности. Аналогично, узлы 7 и 8 фиксируют моменты обработки интеллектуальным узлом коммутации информационных пакетов $r_2 = \overline{2, J}$, $r_3 = \overline{J+1, R}$ и $r_1$, $r_3 = \overline{J+1, R}$ классов приоритетности соответственно.

Узел 9 описывает состояние системы в момент, когда интеллектуальный узел имеет возможность обеспечивать выделенные ресурсы для поступивших информационных пакетов всех классов приоритетности.

Узел 10 отражает момент состояния системы, когда для обработки поступивших информационных пакетов задействованы все $(V_r + K_r)$ коммуникационные ресурсы.

Ветви (1,2), (2,3), (2,4), (2,5), …, (9,10) и соответствующие им *W*-функции ($W_{12}$, $W_{23}$, $W_{24}$, $W_{25}$, …, $W_{9/10}$) описывают параметры (время обработки информационных пакетов $r_1$, $r_2 = \overline{2, J}$ и $r_3 = \overline{J+1, R}$ классов приоритетности, джиттер задержки обработки информационных пакетов $r_1$, $r_2 = \overline{2, J}$ и $r_3 = \overline{J+1, R}$ классов приоритетности, время восстановления отдельных элементов узла коммутации в случае их выхода из строя и др.) характеризующие переходы интеллектуальных узлов коммутации из одного состояния в другое в процессе его функционирования в описанных выше режимах (например, ветвь $W_{12}$ отражает время обработки поступивших информационных пакетов $r_1$, $r_2 = \overline{2, J}$ и $r_3 = \overline{J+1, R}$ классов приоритетности в $V_{r-1}$ обслуживающих устройствах, и т.д.).

Следует заметить, что представленная на рис. 3.3. структурно-логическая *GERT*-модель учитывает факторы внешних воздействий (соответственного возможной потери информационных пакетов) и реальной надежности (возможных отказов оборудования) путем введения ветвей обратных связей с соответствующими им характеристиками (например $W_{42}$, $W_{52}$, ,$W_{74}$, и т.д.).

Представленная, на рис 3.3. структурно-логическая *GERT*-модель, а также анализ ряда работ [28, 57], посвященных исследованию процессов превентивного и конечного управления информационных потоков в интеллектуальном коммутационном оборудовании позволили сформировать характеристики ветвей и параметры распределения в виде, представленном в табл. 3.1.

Таблица 3.1

Характеристики ветвей GERT-модели технологии функционирования интеллектуального узла коммутации ТКС

| № п/п | Ветвь | *W*-функция | Вероятность | Производящая функция моментов |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| 1. | (1,1) | $W_{11}$ | $1\text{-}p_1$ | $\lambda_1/(\lambda_1 - s)$ |
| 2. | (1,2) | $W_{12}$ | $p_1$ | $\lambda_2/(\lambda_2 - s)$ |
| 3. | (2,1) | $W_{21}$ | $1\text{-}p_2\text{-}p_3\text{-}p_4\text{-}p_5$ | $\lambda_1/(\lambda_1 - s)$ |
| 4. | (2,3) | $W_{23}$ | $p_2$ | $\lambda_3/(\lambda_3 - s)$ |
| 5. | (2,4) | $W_{24}$ | $p_3$ | $\lambda_4/(\lambda_4 - s)$ |
| 6. | (2,5) | $W_{25}$ | $p_4$ | $\lambda_5/(\lambda_5 - s)$ |
| 7. | (2,9) | $W_{29}$ | $p_5$ | $\lambda_6/(\lambda_6 - s)$ |
| 8. | (3,2) | $W_{32}$ | $1\text{-}p_6\text{-}p_7\text{-}p_8$ | $\lambda_7/(\lambda_7 - s)$ |
| 9. | (3,6) | $W_{36}$ | $p_6$ | $\lambda_6/(\lambda_6 - s)$ |
| 10. | (3,8) | $W_{38}$ | $p_7$ | $\lambda_8/(\lambda_8 - s)$ |
| 11. | (3,9) | $W_{39}$ | $p_8$ | $\lambda_6/(\lambda_6 - s)$ |
| 12. | (4,2) | $W_{42}$ | $1\text{-}p_9\text{-}p_{10}\text{-}p_{11}$ | $\lambda_7/(\lambda_7 - s)$ |
| 13. | (4,6) | $W_{46}$ | $p_9$ | $\lambda_9/(\lambda_9 - s)$ |
| 14. | (4,7) | $W_{47}$ | $p_{10}$ | $\lambda_{10}/(\lambda_{10} - s)$ |
| 15. | (4,9) | $W_{49}$ | $p_{11}$ | $\lambda_{11}/(\lambda_{11} - s)$ |
| 16. | (5,2) | $W_{52}$ | $1\text{-}p_{12}\text{-}p_{13}\text{-}p_{14}$ | $\lambda_7/(\lambda_7 - s)$ |
| 17. | (5,7) | $W_{57}$ | $p_{12}$ | $\lambda_6/(\lambda_6 - s)$ |
| 18. | (5,8) | $W_{58}$ | $p_{13}$ | $\lambda_6/(\lambda_6 - s)$ |
| 19. | (5,9) | $W_{59}$ | $p_{14}$ | $\lambda_6/(\lambda_6 - s)$ |
| 20. | (6,3) | $W_{63}$ | $1\text{-}p_{15}$ | $\lambda_{12}/(\lambda_{12} - s)$ |
| 21. | (6,9) | $W_{69}$ | $p_{15}$ | $\lambda_{13}/(\lambda_{13} - s)$ |

| | | | | |
|---|---|---|---|---|
| 22. | (7,4) | $W_{74}$ | $1\text{-}p_{16}$ | $\lambda_{12}/(\lambda_{12}-s)$ |
| 23. | (7,9) | $W_{79}$ | $p_{16}$ | $\lambda_{14}/(\lambda_{14}-s)$ |
| 24. | (8,3) | $W_{83}$ | $1\text{-}p_{17}$ | $\lambda_{12}/(\lambda_{12}-s)$ |
| 25. | (8,9) | $W_{89}$ | $p_{17}$ | $\lambda_{15}/(\lambda_{15}-s)$ |
| 26. | (9,2) | $W_{92}$ | $1\text{-}p_{18}$ | $\lambda_{7}/(\lambda_{7}-s)$ |
| 27. | (9,10) | $W_{9/10}$ | $p_{18}$ | $\lambda_{16}/(\lambda_{16}-s)$ |

Следует заметить, что проведенные исследования позволили выявить ряд закономерностей в процессе функционирования интеллектуальных узлов коммутации ТКС, связанных с практически идентичностью показателей и соответственно производящих функций моментов на отдельных этапах и в ряде режимов функционирования. Это в конечном итоге вылилось в уменьшение производящих функций моментов (см. табл. 3.1). Так ветви (1,1) и (2,1) характеризуются производящей функцией моментов $\lambda_1/(\lambda_1-s)$, ветви (2,9), (3,6), (3,9), (5,7), (5,8) и (5,9) производящей функцией моментов $\lambda_6/(\lambda_6-s)$, ветви (3,2), (4,2), (5,2) и (9,2) производящей функцией моментов $\lambda_7/(\lambda_7-s)$, а ветви (6,3), (7,4) и (8,3) производящей функцией моментов $\lambda_{12}/(\lambda_{12}-s)$.

В соответствии с характеристиками ветвей *GERT*-сети определим эквивалентную *W*-функцию времени обработки информационного пакета в интеллектуальном узле коммутации как:

$$W_E(s)=\frac{\left[W_{12}W_{9/10}\begin{pmatrix}W_{29}+W_{23}\left(W_{36}W_{69}+W_{38}W_{89}+W_{39}\right)+\\+W_{24}\left(W_{47}W_{79}+W_{46}W_{69}\right)+W_{25}\left(W_{59}+W_{57}W_{79}+W_{58}W_{89}\right)\end{pmatrix}\right]}{\left[\begin{array}{l}1-W_{11}-W_{12}\times\\ \times\begin{pmatrix}W_{21}-W_{23}\left(W_{32}-W_{36}W_{63}-W_{38}W_{83}-W_{92}\left(W_{36}W_{69}-W_{38}W_{89}-W_{39}\right)\right)-\\-W_{24}\left(W_{42}-W_{47}\left(W_{74}-W_{79}W_{92}\right)-W_{46}\left(W_{63}-W_{69}W_{92}\right)-W_{49}W_{92}\right)-\\-W_{25}\left(W_{52}-W_{58}\left(W_{83}-W_{89}W_{92}\right)-W_{57}\left(W_{74}-W_{79}W_{92}\right)-W_{59}W_{92}\right)-\\-W_{29}W_{92}\end{pmatrix}\end{array}\right]}=$$

Таким образом, разработанная математическая GERT-модель отличается от известных учетом таких факторов:

– использования «облачных» антивирусных ресурсов в случае возможных злоумышленных вирусных вторжений, что характеризуется ветвями (2,3,6,9), (2,3,8,9), (2,4,6,9), (2,5,8,9);

– выхода из строя отдельных элементов интеллектуального узла коммутации (фактора реальной надежности технического изделия), что характеризуется ветвями (3,2), (4,2), (5,2), (9,2).

Анализ данных, представленных в табл. 3.1. показал многоуровневость и высокую структурную сложность разрабатываемой *GERT*-модели. Особенно остро данная проблема фиксируется на участках, сформированных узлами 2-3-4-5-5-6-7-8-9 (ветвей (2,3,6,9), (2,3,8,9), (2,4,7,9), (2,5,8,9)). Поэтому в дальнейшем в работе, используя метод декомпозиции, исследуем наиболее важные параметры, характерные режимам работы интеллектуальных узлов коммутации ТКС в условиях злоумышленных воздействий компьютерных вирусов.

Фактор внешних злоумышленных воздействий особенно четко зафиксирован в той части *GERT*-сети, которая характеризуется узлами (1,2,3,6,8,9,10). Именной поэтому преобразуем общую *GERT*-модель технологии функционирования интеллектуального узла коммутации ТКС (рис. 3.3) в упрощенную *GERT*-сеть узла коммутации в режиме обработки метаданных для «облачных» антивирусных систем (рис. 3.4) (в скобках номера узлов из рис. 3.3.).

В соответствии с характеристиками ветвей *GERT*-сети (см. табл. 3.1.), а так же с учетом того, что функции $W_{36}^{*} = \frac{p_6\lambda_6}{\lambda_6 - s} + \frac{p_9\lambda_9}{\lambda_9 - s}$ и $W_{38}^{*} = \frac{p_7\lambda_8}{\lambda_8 - s} + \frac{p_{13}\lambda_6}{\lambda_6 - s}$ вычислялись в соответствии с методикой эквивалентных упрощающих преобразований (см. подраздел 2.1.1.), определим

эквивалентную *W*-функцию времени обработки информационных пакетов метаданных при их передаче в «облачные» антивирусные системы как:

$$W_E(s) = \frac{W_{36}W_{69} + W_{38}W_{89} + W_{39}}{1 - W_{36}W_{63} - W_{38}W_{83}} =$$

$$= \frac{\left[\begin{array}{l} \left(\begin{array}{l} p_6 p_{15}\lambda_6\lambda_{13}(\lambda_8 - s)(\lambda_9 - s)(\lambda_{15} - s) + p_9 p_{15}\lambda_9\lambda_{13}(\lambda_6 - s)(\lambda_8 - s)(\lambda_{15} - s) + \\ p_8\lambda_6(\lambda_8 - s)(\lambda_9 - s)(\lambda_{13} - s)(\lambda_{15} - s) + p_7 p_{17}\lambda_8\lambda_{15}(\lambda_6 - s)(\lambda_9 - s)(\lambda_{13} - s) + \\ + p_{13} p_{17}\lambda_6\lambda_{15}(\lambda_8 - s)(\lambda_9 - s)(\lambda_{13} - s) \end{array}\right) \times \\ \times (\lambda_{12} - s) \end{array}\right]}{(\lambda_9 - s)(\lambda_{13} - s)(\lambda_{15} - s)\left(\begin{array}{l} (\lambda_6 - s)(\lambda_{12} - s)(\lambda_8 - s) - \\ - p_6 q_1\lambda_6\lambda_{12}(\lambda_8 - s) - p_7 q_2\lambda_8\lambda_{12}(\lambda_6 - s) \end{array}\right)},$$

где $q_1 = 1 - p_{15}$, $q_2 = 1 - p_{17}$.

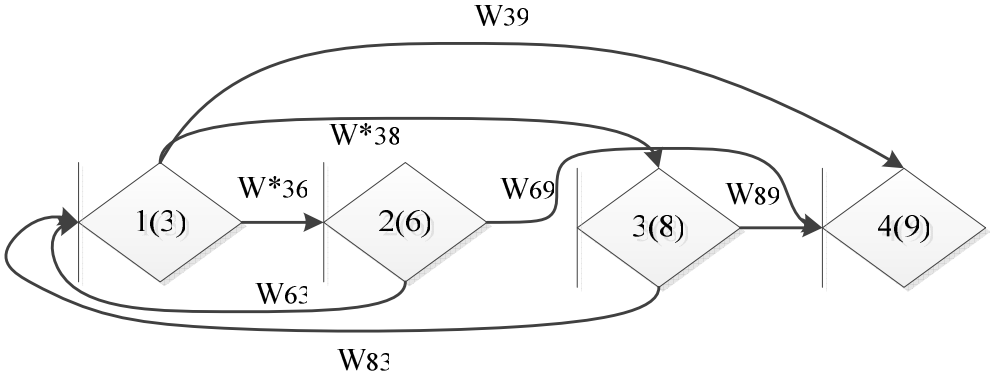



Рис. 3.4. Упрощенная *GERT*-сеть интеллектуального узла коммутации ТКС в режиме обработки метаданных для «облачных» антивирусных систем

Исходя из того, что в сложных *GERT*-сетях с возможными циклами отсутствуют простые методы нахождения особых точек функции $\Phi_E(z)$ замены действительных переменных $(z = -i\varsigma)$, где $\varsigma$ – действительная переменная, выполняя комплексное преобразование, в ходе моделирования получим:

$$\Phi(z) = \frac{\ell z^5 + \rho z^4 + u z^3 + k z^2 + w z + h}{(\lambda_9 + z)(\lambda_{13} + z)(\lambda_{15} + z)\left(z^3 + v z^2 + r z + c\right)}, \qquad (3.6)$$

где $\ell = p_8\lambda_6$,

$$\rho = \begin{bmatrix} p_6p_{15}\lambda_6\lambda_{13} + p_9p_{15}\lambda_9\lambda_{13} + p_8\lambda_6\left(\lambda_8 + \lambda_9 + \lambda_{13} + \lambda_{15}\right) + p_7p_{17}\lambda_8\lambda_{15} + \\ + p_{13}p_{17}\lambda_6\lambda_{15} \end{bmatrix},$$

$$u = \begin{bmatrix} p_6p_{15}\lambda_6\lambda_{13}\left(\lambda_8 + \lambda_9 + \lambda_{12} + \lambda_{15}\right) + p_9p_{15}\lambda_9\lambda_{13}\left(\lambda_6 + \lambda_8 + \lambda_{12} + \lambda_{15}\right) + \\ + p_8\lambda_6\left(\begin{matrix}\lambda_8\lambda_{12} + \lambda_9\lambda_{12} + \lambda_{12}\lambda_{13} + \lambda_{12}\lambda_{15} + \lambda_8\lambda_9 + \lambda_8\lambda_{13} + \\ + \lambda_9\lambda_{13} + \lambda_8\lambda_{15} + \lambda_9\lambda_{15} + \lambda_{13}\lambda_{15}\end{matrix}\right) + \\ + p_7p_{17}\lambda_8\lambda_{15}\left(\lambda_6 + \lambda_9 + \lambda_{12} + \lambda_{13}\right) + p_{13}p_{17}\lambda_6\lambda_{15}\left(\lambda_8 + \lambda_9 + \lambda_{12} + \lambda_{13}\right) \end{bmatrix},$$

$$k = \begin{bmatrix} p_6p_{15}\lambda_6\lambda_{13}\left(\lambda_8\lambda_9 + \lambda_8\lambda_{12} + \lambda_9\lambda_{12} + \lambda_{12}\lambda_{15} + \lambda_8\lambda_{15} + \lambda_9\lambda_{15}\right) + \\ + p_9p_{15}\lambda_9\lambda_{13}\left(\lambda_6\lambda_{12} + \lambda_8\lambda_{12} + \lambda_{12}\lambda_{15} + \lambda_6\lambda_{15} + \lambda_8\lambda_{15} + \lambda_6\lambda_8\right) + \\ + p_8\lambda_6\left(\begin{matrix}\lambda_{12}\lambda_{13}\lambda_{15} + \lambda_8\lambda_{12}\lambda_{15} + \lambda_9\lambda_{12}\lambda_{15} + \lambda_8\lambda_{12}\lambda_{13} + \lambda_9\lambda_{12}\lambda_{13} + \\ + \lambda_8\lambda_9\lambda_{12} + \lambda_8\lambda_{13}\lambda_{15} + \lambda_9\lambda_{13}\lambda_{15} + \lambda_8\lambda_9\lambda_{15} + \lambda_8\lambda_9\lambda_{13}\end{matrix}\right) + \\ + p_7p_{17}\lambda_8\lambda_{15}\left(\lambda_6\lambda_{12} + \lambda_9\lambda_{12} + \lambda_{12}\lambda_{13} + \lambda_6\lambda_{13} + \lambda_9\lambda_{13} + \lambda_6\lambda_9\right) + \\ + p_{13}p_{17}\lambda_6\lambda_{15}\left(\lambda_8\lambda_{12} + \lambda_9\lambda_{12} + \lambda_{12}\lambda_{13} + \lambda_8\lambda_{13} + \lambda_9\lambda_{13} + \lambda_8\lambda_9\right) \end{bmatrix},$$

$$w = \begin{bmatrix} p_6p_{15}\lambda_6\lambda_{13}\left(\lambda_8\lambda_9\lambda_{15} + \lambda_8\lambda_{12}\lambda_{15} + \lambda_9\lambda_{12}\lambda_{15} + \lambda_8\lambda_9\lambda_{12}\right) + \\ + p_9p_{15}\lambda_9\lambda_{13}\left(\lambda_6\lambda_{12}\lambda_{15} + \lambda_8\lambda_{12}\lambda_{15} + \lambda_6\lambda_8\lambda_{15} + \lambda_6\lambda_8\lambda_{12}\right) + \\ + p_8\lambda_6\left(\begin{matrix}\lambda_8\lambda_9\lambda_{13}\lambda_{15} + \lambda_8\lambda_{12}\lambda_{13}\lambda_{15} + \lambda_9\lambda_{12}\lambda_{13}\lambda_{15} + \lambda_8\lambda_9\lambda_{12}\lambda_{15} + \\ + \lambda_8\lambda_9\lambda_{12}\lambda_{13}\end{matrix}\right) + \\ + p_7p_{17}\lambda_8\lambda_{15}\left(\lambda_6\lambda_{12}\lambda_{13} + \lambda_9\lambda_{12}\lambda_{13} + \lambda_6\lambda_9\lambda_{12} + \lambda_6\lambda_9\lambda_{13}\right) + \\ + p_{13}p_{17}\lambda_6\lambda_{15}\left(\lambda_8\lambda_{12}\lambda_{13} + \lambda_9\lambda_{12}\lambda_{13} + \lambda_8\lambda_9\lambda_{12} + \lambda_8\lambda_9\lambda_{13}\right) \end{bmatrix},$$

$$h = \begin{bmatrix} p_6p_{15}\lambda_6\lambda_{13}\lambda_8\lambda_9\lambda_{12}\lambda_{15} + p_9p_{15}\lambda_9\lambda_{13}\lambda_6\lambda_8\lambda_{12}\lambda_{15} + \\ + p_8\lambda_6\lambda_8\lambda_9\lambda_{12}\lambda_{13}\lambda_{15} + p_7p_{17}\lambda_8\lambda_{15}\lambda_6\lambda_9\lambda_{12}\lambda_{13} + p_{13}p_{17}\lambda_6\lambda_{15}\lambda_8\lambda_9\lambda_{12}\lambda_{13} \end{bmatrix},$$

$$v = \lambda_8 + \lambda_6\lambda_{12} + \lambda_6 + \lambda_{12},$$

$$r = \lambda_6\lambda_8 + \lambda_8\lambda_{12} - \lambda_6\lambda_{12} - p_7q_2\lambda_8\lambda_{12},$$

$$c = \lambda_6\lambda_8\lambda_{12} - p_6q_1\lambda_6\lambda_{12} - p_7q_2\lambda_6\lambda_8\lambda_{12}.$$

Плотность распределения вероятностей времени обработки информационных пакетов метаданных:

$$\varphi(x)=\frac{1}{2\pi i}\int_{-i\infty}^{i\infty}e^{zx}\frac{\ell z^5+\rho z^4+uz^3+kz^2+wz+h}{(\lambda_9+z)(\lambda_{13}+z)(\lambda_{15}+z)(z^3+vz^2+rz+c)}dz, \qquad (3.7)$$

где интегрирование выполняется по контуру Бромвича.

Способ интегрирования зависит от того, имеет ли функция $\Phi(z)$, только простые полюсы, или полюсы некоторого порядка. В том случае, когда функция $\Phi(z)$ имеет только простые полюсы, выражение $e^{zx}\Phi(z)$ можно представить в виде:

$$e^{zx}\Phi(z)=\frac{e^{zx}\left(\ell z^5+\rho z^4+uz^3+kz^2+wz+h\right)}{z^6+z^5g_5+z^4g_4+z^3g_3+z^2g_2+zg_1+g_0}, \qquad (3.8)$$

где

$$g_5=v+y_1,$$

$$g_4=r+v(y_1+y_2),$$

$$g_3=c+ry_1+vy_2+y_3,$$

$$g_2=c(y_1+ry_2+vy_3),$$

$$g_1=cy_2+ry_3,$$

$$g_0=cy_3,$$

$$y_1=\lambda_9+\lambda_{13}+\lambda_{15},$$

$$y_2=\lambda_9\lambda_{13}+\lambda_9\lambda_{15}+\lambda_{13}\lambda_{15},$$

$$y_3=\lambda_9\lambda_{13}\lambda_{15}.$$

Тогда плотность распределения времени передачи файла

$$\varphi(z)=\sum_{k=1}^{6}Res_{z=z_k}\left[e^{zx}\Phi(z)\right]=\sum_{k=1}^{6}\frac{e^{z_kx}\left(\ell z_k^5+\rho z_k^4+uz_k^3+kz_k^2+wz_k+h\right)}{6z_k^5+5z_k^4g_5+4z_k^3g_4+3z_k^2g_3+2z_kg_2+g_1}. \qquad (3.9)$$

Функция $\Phi(z)$ кроме простых полюсов, определяемых корнями уравнения $z^3+vz^2+rz+c=0$, может иметь и полюсы второго или третьего

порядка. Это возможно в тех случаях, когда значения $\lambda_9$, $\lambda_{13}$ и $\lambda_{15}$ или совпадают между собой, или равны значениям корней $z_4$, $z_5$, $z_6$.

В этих случаях плотность распределения времени обработки информационных пакетов метаданных при их передаче в «облачные» антивирусные системы $\varphi_b(x)$ находится по формуле нахождения вычетов $t_{-1}$ от полюсов $z_k$ порядка $n$:

$$t_{-1} = \frac{1}{(n-1)!} \lim_{z \to z_k} \frac{d^{n-1}\left[(z - z_k)^n e^{zk} \Phi(z)\right]}{dz^{n-1}}.$$

Выражение (3.6) представляет собой дробно-рациональную функцию относительно $z$ со степенью знаменателя большей, чем степень числителя, поэтому для него выполняются условия леммы Жордана [23]. Функция $\Phi(z)$ имеет полюсы в точках $z_1 = -\lambda_9$, $z_2 = -\lambda_{13}$, $z_3 = -\lambda_{15}$. Многочлен $z^3 + vz^2 + rz + c$ формирует еще три полюса.

Решение уравнения

$$z^3 + vz^2 + rz + c = 0 \qquad (3.10)$$

может быть найдено любым численным методом. В итоге получим еще три особые точки ($z_4$, $z_5$, $z_6$).

Аналогично подразделу 2.2. используя специализированный математический пакет *Mathcad*, определим простые полюсы $z$ функции $\Phi(z)$ и найдем плотность распределения вероятностей $\varphi(x)$ времени обработки информационных пакетов метаданных при их передаче в «облачные» антивирусные системы. При этом в качестве начальных данных определим следующие параметры ветвей *GERT*-сети:

$$p_6 = 0{,}9995,\ p_7 = 0{,}9995,\ p_8 = 0{,}9,\ p_9 = 0{,}9995,$$

$$p_{13} = 0{,}9995,\ p_{15} = 0{,}9,\ p_{17} = 0{,}9$$

$$\lambda_6 = \{0{,}47;\ 0{,}57;\ \ldots;0{,}97\},\ \lambda_8 = 0{,}37,\ \lambda_9 = 0{,}991,\ \lambda_{12} = 0{,}6,\ \lambda_{13} = 0{,}6,\ \lambda_{15} = 0{,}87.$$

На рис. 3.5 и 3.6 представлены графики кривых функции распределения $\Phi(x)$ и плотности распределения $\varphi(x)$ вероятностей времени обработки информационных пакетов метаданных в интеллектуальном узле коммутации при их передаче в «облачные» антивирусные системы для приведенных выше условий.

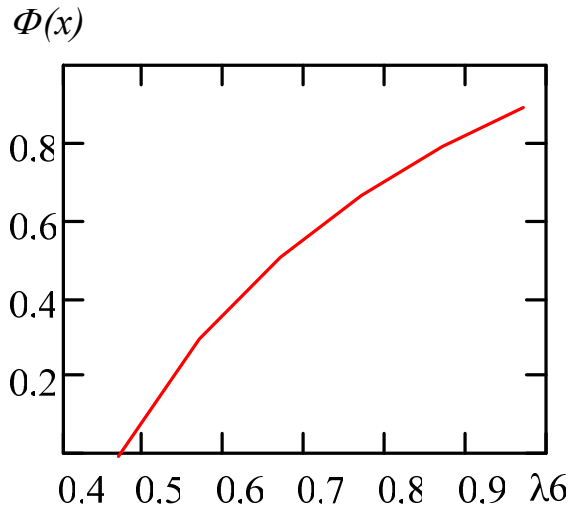



Рис. 3.5. График функции распределения $\Phi(x)$


Рис. 3.6. Плотность распределения времени обработки информационных пакетов метаданных при их передаче в «облачные» антивирусные системы

Внешний вид кривых графиков рис. 3.5 и 3.6 дает основания предположить, что случайная величина времени обработки информационных пакетов метаданных в интеллектуальном узле коммутации при их передаче в «облачные» антивирусные системы имеет гамма-распределение.

Кроме того, как видно из рис. 3.5. максимальное значение произвольной функции распределения $\Phi(x)$ для заданных условий достигает единицы. При этом рис 3.6. фиксирует, что максимум плотности распределения времени обработки информационных пакетов метаданных приходится на малый промежуток от 1 до 2 мс.

Таким образом, на основе GERT-сети разработана математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета, которая отличается от известных учетом максимальной приоритезации информационных пакетов метаданных при их передаче в «облачные» антивирусные системы.

## 3.2. Усовершенствованный алгоритм управления доступом к облачным телекоммуникационным ресурсам

Для решения поставленной в первом разделе оптимизационной задачи повышения оперативности обработки информационных пакетов, в интеллектуальных узлах коммутации при их передаче в «облачные» антивирусные системы предлагается усовершенствовать алгоритм управления доступом к соответствующим «облачным» телекоммуникационным ресурсам. В основу рассматриваемого алгоритма положена процедура вычисления виртуального времени обработки информационных пакетов, отличающаяся от известных учетом фактора введения дополнительного уровня приоритезации для информационных пакетов метаданных [28, 68]. При этом указанные информационные пакеты

получают наивысший приоритет обработки в интеллектуальных узлах коммутации класса $r_1$.

В табл. 3.2. представлены допустимые значения среднего времени и джиттера времени обработки информационных пакетов различного уровня приоритетности в интеллектуальных узлах коммутации.

Таблица 3.2

Допустимые значения среднего времени и джиттера времени обработки информационных пакетов различного уровня приоритетности

| Уровень приоритета | $r_3 = \overline{J+1, R}$ | $r_2 = \overline{2, J}$ | $r_1 = 1$ |
|---|---|---|---|
| $T_{доп}^{[i]}$, мс | 100-800 | 50-150 | 1-10 |
| $J_{доп}^{[i]}$, мс | 47-53 | 10-30 | 1-5 |

Структурная схема алгоритма управления доступом к «облачным» телекоммуникационным ресурсам представлена на рис. 3.7.

На первом шаге в рассматриваемой структурной схеме осуществляется проверка нахождения пакетов на входе интеллектуального узла коммутации. При их отсутствии – алгоритм переходит в режим ожидания поступающих пакетов.

В случае, когда на вход интеллектуального узла коммутации информационные пакеты поступили (всех уровней приоритезации или только отдельных) необходимо выполнить выбор из каждой очереди буфера памяти интеллектуального узла коммутации (см. рис. 3.2.) по одному первому пакету $r_1 = 1$, $r_2 = \overline{2, J}$ и $r_3 = \overline{J+1, R}$ уровня приоритетности для определения «эталонного» информационного пакета с соответствующим уровнем приоритетности. Это позволит сократить время обработки информационных пакетов метаданных при обеспечении заданных показателей оперативности обработки информационных пакетов других уровней приоритетности.

На четвертом шаге рассматриваемом алгоритме определяется значение *VST* и *VFT*. Далее приступаем к выполнению процедур выявления

информационного пакета для обработки в обслуживающем устройстве интеллектуального узла коммутации. При этом учитывается следующее: на вход буферного устройства может поступать $N$ пакетов ($N$ – количество очередей в системе) $r_1$, $r_2$ и $r_3$ уровней приоритетности.

Если значение VST наступило, то на шаге 6 из информационного потока выбирается первый («эталонный») пакет, с некоторым $N_{приор}$, а также значением виртуального времени обслуживания в очереди – $VFT$.

Далее на шаге 9 структурной схемы производится сравнение «эталонного» информационного пакета с другими поступившими на данный момент времени.

При этом решение о присвоении «эталонного» приоритета информационному пакету принимается по следующим критериям:

1) минимальное значение виртуального времени обслуживания в очереди ($VFT = min$);

2) принадлежность информационного пакета к очереди с максимальным приоритетом ($r_1 > r_2 > r_3$).

Следует заметить, что условие присвоения «эталонного» приоритета на шаге 14 выполняется не в полном объеме, а с некоторыми исключениями, определяемыми заранее заданным показателем, например показателем $P_{присв}$ – вероятности присвоения приоритета. Данный показатель может быть определен эмпирическим путем. При этом процедура управления с помощью данного показателя является отличительной особенностью рассматриваемого алгоритма управления доступом к «облачным» телекоммуникационным ресурсам. Данные исключения необходимы для обеспечения качества обслуживания информационных пакетов других (низших) приоритетов.

Информационные пакеты можно сравнивать попарно, при этом в начальный момент времени первый выбранный информационный пакет условно обладает высшим уровнем приоритетности.

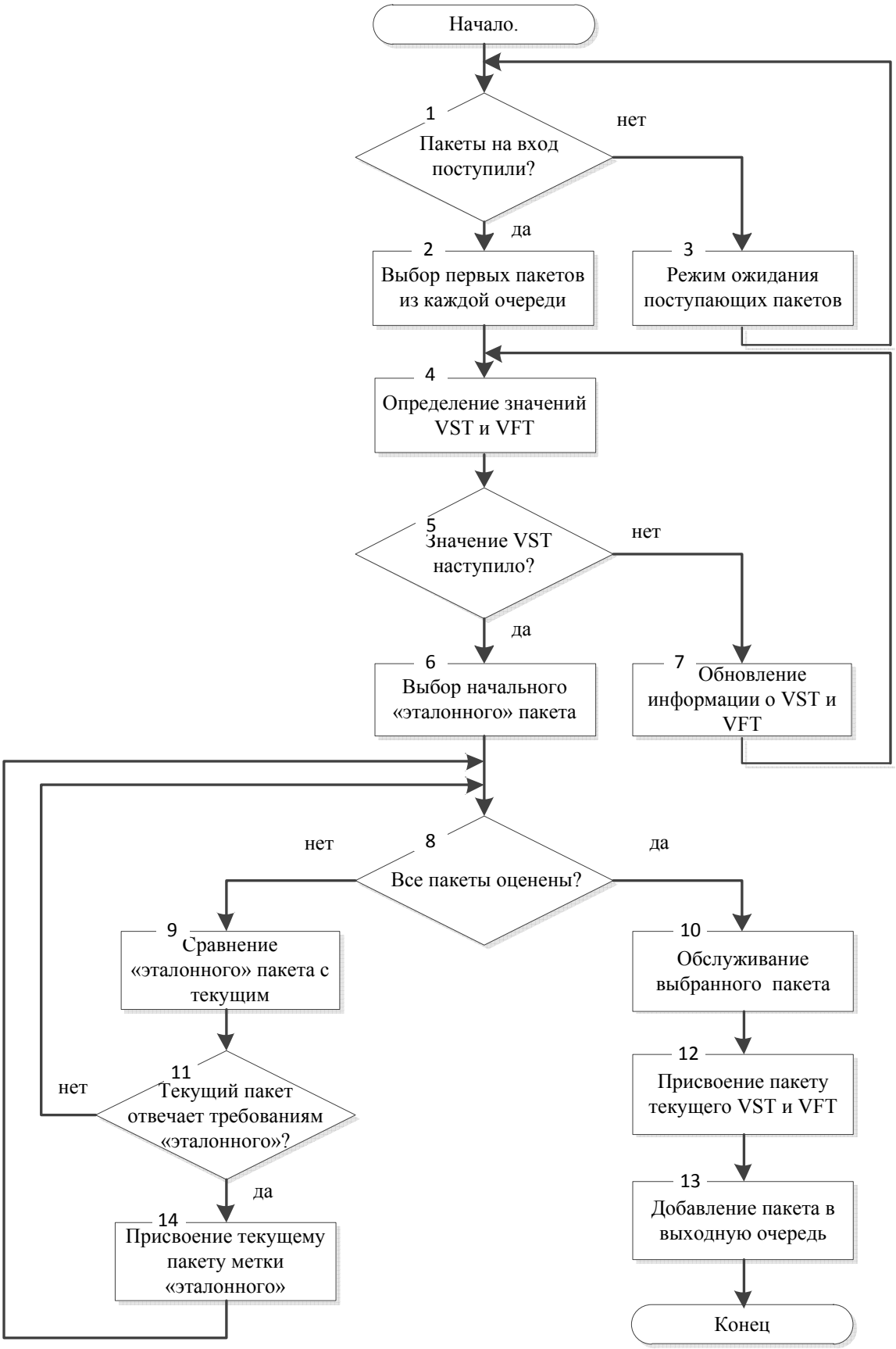



Рис. 3.7. Структурная схема алгоритма управления доступом к «облачным» телекоммуникационным ресурсам

Если условие, определяемое на шаге 5, не наступило, то на шаге 7 алгоритма происходит обновление информации о *VST* и *VFT*.

На шаге 10 происходит переход непосредственно к процедурам обработки информационных пакетов. На шаге 12 информационному пакету присваиваются текущие значения *VST* и *VFT* с целью дальнейшего сопровождения информационного пакета к пункту назначения.

Далее на шаге 13 информационный пакет добавляется в выходную очередь и заканчивается процесс его обработки в интеллектуальном узле коммутации.

Таким образом, разработан алгоритм управления доступом к «облачным» телекоммуникационным ресурсам отличительной особенностью которого является введение нестандартных условий принятия решения о присвоении «эталонного» приоритета информационному пакету на основе дополнительного показателя – вероятности присвоения приоритета. Это позволило решить задачу минимизации времени обработки информационных пакетов метаданных при их передаче в «облачные» антивирусные системы при обеспечении заданного качества обслуживания других информационно-телекоммуникационных услуг.

## Выводы по разделу 3

В разделе разработан метод управления доступом в интеллектуальных узлах коммутации включающий в себя математическую модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета и усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам. Отличительной особенностью метода является комплексное использование стандартных критериев управления информационными потоками в интеллектуальных узлах коммутации с дополнительными, учитывающими

возможность обслуживания информационных пакетов метаданных при их передаче в «облачные» антивирусные системы.

Основными результатами третьего раздела являются:

На основе GERT-сети разработана математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета, отличающаяся от известных учетом максимальной приоритезации информационных пакетов метаданных при их передаче в «облачные» антивирусные системы. Это позволило определить эквивалентную W-функцию, функцию распределения и плотность распределения времени обслуживания информационных пакетов метаданных в интеллектуальных узлах коммутации при их передаче в «облачные» антивирусные системы. В результате проведенных исследований отмечено, что максимум плотности распределения времени обработки информационных пакетов метаданных в интеллектуальных узлах коммутации приходится на малый промежуток от 1 до 2 мс.

Разработан алгоритм управления доступом к «облачным» телекоммуникационным ресурсам, отличающийся от известных введением нестандартных условий принятия решения о присвоении «эталонного» приоритета информационному пакету на основе дополнительного показателя – вероятности присвоения приоритета. Это дает возможность решить задачу минимизации времени обработки информационных пакетов метаданных при их передаче в «облачные» антивирусные системы при обеспечении заданного качества обслуживания других информационно-телекоммуникационных услуг.

Основные научные результаты, изложенные в третьем разделе, опубликованы в работах автора [33, 34, 37, 38, 39, 40, 41, 45, 46, 47, 48].

# РАЗДЕЛ 4
# ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ РАЗРАБОТАННОГО МЕТОДА И ОБОСНОВАНИЕ ПРАКТИЧЕСКИХ РЕКОМЕНДАЦИЙ ПО ЕГО ИСПОЛЬЗОВАНИЮ

В разделе производится выбор показателя эффективности управления доступом к облачным антивирусным телекоммуникационным ресурсам. На основе результатов математического и имитационного моделирования проводится выбор показателя вероятности присвоения приоритета для определения «эталона» приоритета и оценка эффективности метода управления доступом к облачным телекоммуникационным ресурсам для обеспечения антивирусной защиты данных. Обосновывается достоверность результатов математического моделирования, и предлагаются практические рекомендации по использованию разработанного метода.

## 4.1. Обоснование выбора показателя эффективности управления доступом к облачным антивирусным телекоммуникационным ресурсам

В диссертационной работе было описано достаточно широкий спектр показателей качества обслуживания, которые в совокупности представляют собой некоторую функцию, отражающую свойство антивирусной безопасности системы с одной стороны, а с другой стороны характеризующую эффективность функционирования ТКС. К их числу относятся следующие показатели качества обслуживания, которые согласно рекомендации МСЭ-Т G.1010 рассматриваются как наиболее важные:

– производительность сети;

– потери пакетов;

– время передачи данных;

– вариация задержки (джиттер).

В первом разделе было определена возможность каждого из приведенных показателей влияния на выбранную функцию характеризующую выполнение требований информационной и функциональной безопасности в случае воздействия на систему злоумышленного программного обеспечения – $B_i^{(TKC)}$.

В то же время в условиях использования облачных средств антивирусного программного обеспечения на приведенную функцию безопасности в большей степени влияют показатели производительности сети, время передачи данных и вероятность потери пакетов.

Под производительностью ТКС понимается свойство сети обеспечивать с заданными вероятностно-временными характеристиками качества обслуживания передачу от отправителей к получателям требуемого объёма данных [68].

Проведенные исследования показали, что к основным показателям производительности сети относят эффективную, пиковую, устойчивую и минимальную скорости передачи, измеряемые, как правило, в бит/с. Для упрощения диссертационных исследований определим, что минимальное значение производительности обычно гарантируется поставщиком услуг, который, в свою очередь, должен иметь гарантии от сетевого провайдера. Параметры, связанные с эффективной скоростью передачи могут быть определены через дескриптор трафика *IP*-сети, который описан в рекомендации МСЭ-Т *Y. 1221* [91].

В ходе исследования необходимо учитывать влияние потерь пакетов, которые, как правило, вызваны не столько ошибками передающей среды, сколько возможными перегрузками в сети по пути следования данных. Значительный уровень потерь пакетов приводит к падению общей производительности сети и, как следствие, к неудовлетворительному качеству работы приложений. Количественно чувствительность к потерям и ошибкам оценивается через следующие показатели:

– коэффициент потерь пакетов *IP* (*IP packet loss ratio, IPLR*);

– коэффициент ошибок пакетов *IP* (*IP packet error ratio, IPER*).

Учет и оценка данного показателя наиболее наглядно демонстрируют преимущества того или иного метода управления телекоммуникационными ресурсами $r_2 = \overline{2, J}$ и $r_3 = \overline{J+1, R}$ уровней приоритетности. Но поскольку в рамках диссертационного исследования большее внимание уделяется обслуживанию информационных пакетов $r_1$ уровня приоритетности оценивать эффективность разработанного метода целесообразнее по следующему показателю – показателю времени передачи информационных пакетов.

В соответствии с рекомендациями МСЭ-Т Y. 1540 [91] время передачи пакетов является основным параметром, характеризующим доставку пакетов *IP*-сети, и выражается через параметр задержки *IPTD* (*IP packet transfer delay*), который определяется как время доставки пакета между источником и получателем для всех пакетов – как успешно переданных, так и пакетов с ошибками.

Из ряда научных работ [1, 4, 8, 27, 62] известно, что одной из основных составляющих времени передачи информационных пакетов является время ожидания в очереди и время обслуживания информационных пакетов (далее оба показателя объединим в общее время обработки) в интеллектуальных узлах коммутации. В условиях использования облачных антивирусных систем данный показатель во многом определяет уровень информационной и функциональной безопасности как отдельных средств телекоммуникации так и ТКС в целом

Именно поэтому с целью оценки эффективности разработанных алгоритмов и метода было проведено их сравнение с ранее известным, наиболее эффективным решением (алгоритмом управления очередями в многопротокольных интеллектуальных маршрутизаторах $WF^2Q$), как с уже получившими протокольную реализацию. При этом количественный анализ

адекватности разработанных моделей управления трафиком проводился путём сравнения результатов аналитического, имитационного моделирования и натурного эксперимента.

## 4.2. Разработка имитационной модели системы управления доступом к облачным телекоммуникационным ресурсам

Одним из ключевых этапов диссертационного исследования является синтез полученных знаний в единую систему антивирусной защиты данных и разработка имитационной модели данной системы. При этом их целью должно быть решение следующих частных задач:

– проверка адекватности разработанных моделей и метода управления доступом к облачным телекоммуникационным ресурсам;

– анализ достоверности полученных результатов в ходе решения поставленных оптимизационных задач;

– обоснованный выбор показателей, коэффициентов и характеристик функционирования системы, а также оценка по ним эффективности разработанного метода;

– выработка научно-практических рекомендаций по использованию моделей и метода управления доступом к облачным телекоммуникационным ресурсам в современных и перспективных информационных системах.

Для обоснования достоверности полученных результатов и оценки эффективности метода управления доступом к облачным телекоммуникационным ресурсам было проведено имитационное моделирование. В качестве инструментария имитационного моделирования использовано среду символьной математики *MathCAD* – 14, специализированные программы распределения доступа в мультисервисных маршрутизаторах для передачи сигнатур и данных [68, 113, 114].

Обобщенная структурная схема разработанной имитационной модели систем формирования требований к информационной безопасности ТКС и защиты от злоумышленного программного обеспечения представлена на рис. 4.1.

Как видно из рисунка в состав программного комплекса имитационного моделирования входят две системы, выполняющие отдельные функции:

– выбора показателей, ограничений и критериев оптимизации процесса доставки метаданных в облачные антивирусные системы, а также выработки соответствующих управляющих сигналов (команд);

– определения допустимых вероятностно-временных характеристик передачи и обработки метаданных в облачных антивирусных системах

– выработки решений о способах защиты данных и оптимального управления коммутационными ресурсами в процессе передачи метаданных в облачные антивирусные системы.

Следует заметить, что для генерации злоумышленного программного обеспечения использовалось несколько известных генераторов: *«Generator DAT Virusov», «Raptor Virus Generator», Nowhere Man «Virus Creation Laboratory» и др.*

В процессе формирования требований к информационной безопасности ТКС и допустимых вероятностно-временных показателей передачи и обработки метаданных в облачных антивирусных системах эмулировались и рассматривались различные характеристики информационного обмена, типы системного программного обеспечения, различные способы архитектурного построения ТКС. В частности рассматривались такие варианты:

– разнотиповость операционных систем;

– связность сети, количество функциональных узлов и связи между ними;

– интенсивность информационного обмена.

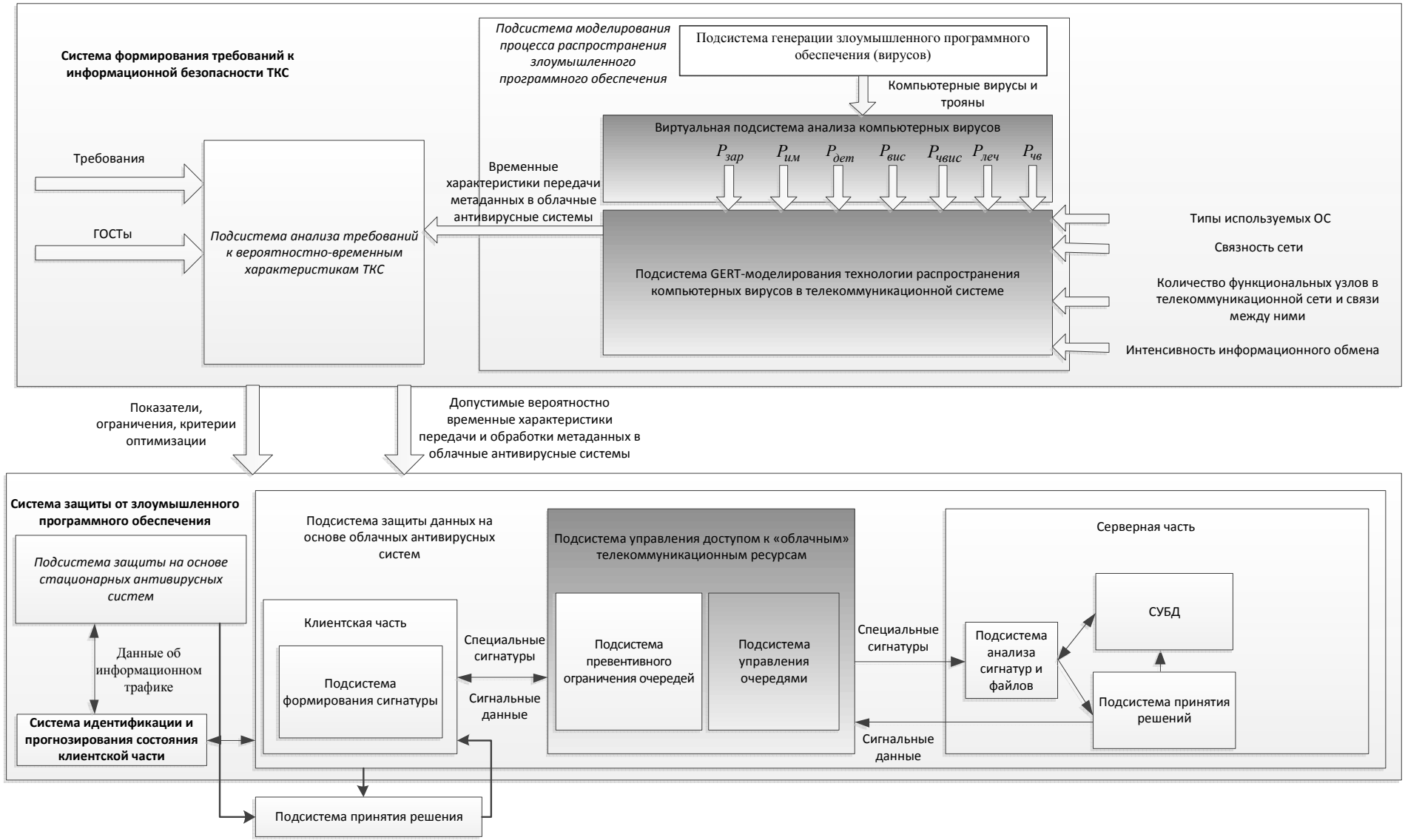



Рис. 4.1. Структурная схема имитационной модели систем формирования требований к информационной безопасности ТКС и защиты от злоумышленного программного обеспечения

Сбор входной информации о загрузке сетевого устройства осуществлялся с помощью стандартного программного анализатора трафика («*Wireshark*»).

Система защиты от злоумышленного программного обеспечения основывается на следующих типах антивирусных программ:

– стационарные;

– облачные.

На рис. А1 и А2 приложения А представлены диаграмма последовательностей процедур информационного обмена с облачными антивирусными системами и диаграмма классов в разработанном программном комплексе соответственно.

Разработка и исследование механизмов антивирусной защиты для стационарных систем не является содержанием диссертационной работы. Для этого могут использоваться известные антивирусные программы (*Антивирус Касперского, Vicrosoft Security Esentiale, Panda, Dr Web, Avira AntiVir* и др.) [23-25].

Одной из наиболее важных составляющих подсистемы защиты на основе облачных антивирусных систем является подсистема управления доступом к облачным телекоммуникационным ресурсам. В ней реализованы основные алгоритмы управления интеллектуальным коммутаторами.

## 4.3. Сравнительные исследования и оценка эффективности метода управления доступом к облачным телекоммуникационным ресурсам для обеспечения антивирусной защиты данных

### 4.3.1 Выбор показателя вероятности присвоения приоритета для определения «эталона» приоритета

Как было указано в подразделе 3.2. для решения задачи управления доступом к «облачным» телекоммуникационным ресурсам необходимо

заранее задать показатель вероятности присвоения приоритета – $P_{присв}$. Для решения данной задачи было проведено ряд экспериментов в условиях, когда $N$ – число независимых потоков информационного трафика (может определяться количеством узлов в ТКС) равно 120, $P$ – пропускная способность канала связи – 10 Гбит/с, *RTT (Round Trip Time)* – время прохождения сигнала от источника трафика до маршрутизатора и обратно равно 100 мс. Тогда $B$ – объем буфера интеллектуального узла коммутации равен:

$$B \approx \frac{P \cdot RTT}{\sqrt{N}}, \tag{4.1}$$

Путем несложных вычислений определим, что объем $B$ равен 12,5 Мб.

Если размер одного информационного пакета 1024 байт [68], то объем буфера интеллектуального узла коммутации ~ 10000 пакетов.

На основе экспертных оценок определено, что вероятность $P_{присв}$ целесообразно выбирать в диапазоне $\{0,5 \ldots 0,9\}$ (в диссертационной работе в качестве примера были выбраны значения 0,7 и 0,9.

### 4.3.2. Оценка эффективности метода управления доступом к облачным телекоммуникационным ресурсам для обеспечения антивирусной защиты данных

Построим графики среднего времени обработки информационного пакета. При этом для распределения информационных пакетов по приоритетам в соответствии с моделью $r_1 = 1$, $r_2 = \overline{2, J}$ и $r_3 = \overline{J+1, R}$, определим, что $J = 4$ а $R = 8$. В соответствии с указанными данными распределение информационных пакетов по их приоритетности представлено таблица 4.1.

Рассмотрим различные варианты распределения на примере использования разработанного алгоритма управления доступом к «облачным» телекоммуникационным ресурсам.

Таблица 4.1

Распределение информационных пакетов по их приоритетности

| Номер приоритета: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Количество пакетов $(\times 1000)$: | 0,5 | 1,2 | 1,2 | 1,2 | 1,4 | 1,4 | 1,4 | 1,4 |

Анализ алгоритмов распределения ресурсов в интеллектуальных узлах коммутации показал, что императивный (статический) подход настройки сетевого оборудования является одним из самых распространенных. Пример распределения телекоммуникационных ресурсов в соответствии с таким подходом администрирования представлен в табл. 4.2.

Таблица 4.2

Пример императивного администрирования и распределения телекоммуникационных ресурсов

| Номер приоритета: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Весовой коэффициент: | 0,35 | 0,15 | 0,15 | 0,15 | 0,05 | 0,05 | 0,05 | 0,05 |

Результаты анализа показателя времени обработки информационных пакетов в интеллектуальном узле коммутации в условиях использования известного ($WF^2Q$) и усовершенствованного алгоритма управления доступом к «облачным» телекоммуникационным ресурсам представлены в виде гистограммы на рис. 4.2.

Как видно из рис. 4.2 использование разработанного алгоритма управления ($P_{присв} = 0{,}9$) в условиях, приведенных в табл. 4.1 и таблица 4.2 до 3 раз уменьшит время обработки информационных пакетов первого уровня приоритетности. В то же время эффективность

усовершенствованного алгоритма управления на всем выбранном диапазоне $P_{присв}$ незначительно уступает эффективности алгоритма $WF^2Q$. Поэтому можно сделать вывод о соизмеримости показателя времени обработки информационных пакетов $r_2 = \overline{2,J}$ и $r_3 = \overline{J+1,R}$ уровней приоритетности.

Таким образом, принцип несправедливого распределения вычислительных и телекоммуникационных ресурсов существенно уменьшает время обработки информационных пакетов выделенного (максимального) уровня приоритетности. Однако при этом наблюдается незначительное ухудшение качества обслуживания информационных пакетов других приоритетов.

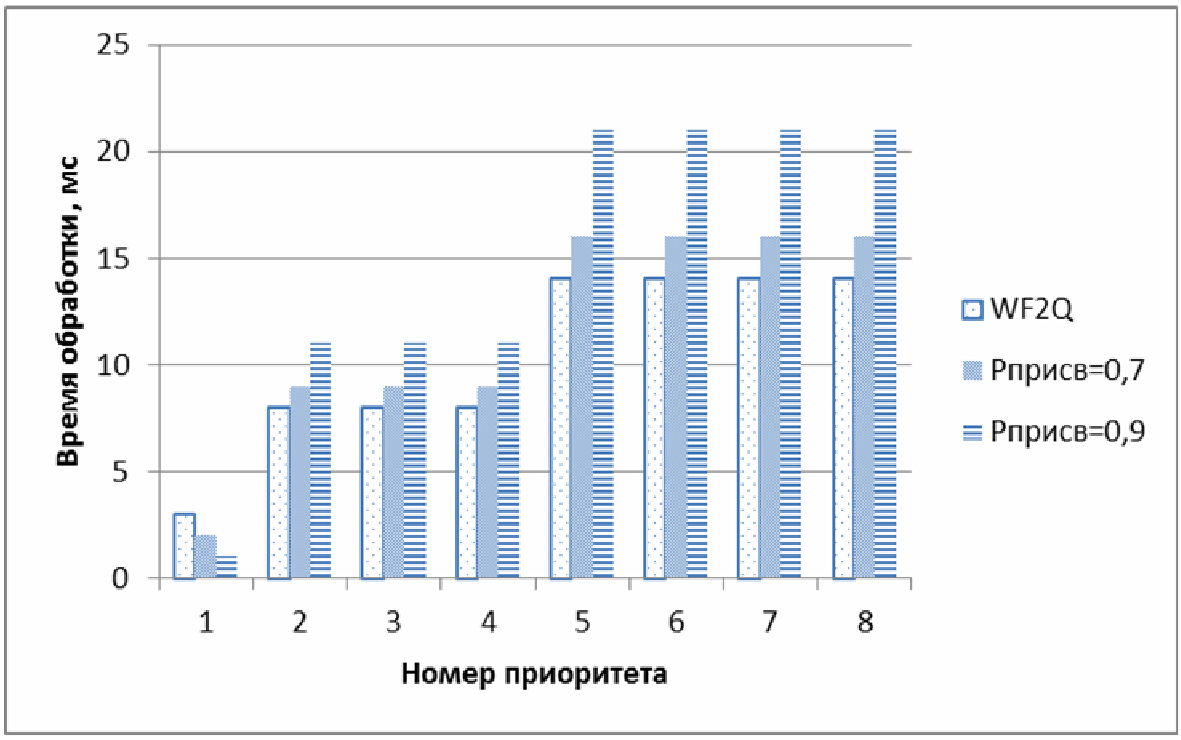



Рис. 4.2. Гистограммы времени обработки информационных пакетов в условиях императивного администрирования

В качестве еще одного примера решения задачи распределения телекоммуникационных ресурсов интеллектуальных узлов коммутации можно отметить принцип справедливого распределения. Анализ алгоритмов справедливого распределения показал наличие различных подходов

определения весовых коэффициентов, определяющих долю обслуживаемого информационного потока. Так одним из примеров является подход, основанный на вычислении весового коэффициента $\omega_i$ с помощью выражения:

$$\omega_i = \frac{\sqrt{i}}{\sum_{j=1}^{N}\sqrt{j}}, N = 8, i = \overline{1..N} \quad (4.2)$$

Значения весовых коэффициентов, полученных с помощью данного выражения представлены в табл. 4.3.

Таблица 4.3

Экспериментальные значения весовых коэффициентов справедливого распределения

| Номер приоритета: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Весовой коэффициент: | 0,17 | 0,16 | 0,15 | 0,14 | 0,12 | 0,11 | 0,09 | 0,06 |

Результаты исследования показателя времени обработки информационных пакетов представлены на рис. 4.3.

Как видно из этого рисунка, использование в усовершенствованном алгоритме управления доступом к «облачным» телекоммуникационным ресурсам принципа справедливого распределения в соответствии с выражением (4.3) позволило до 2 раз при $P_{присв} = 0{,}9$, до 1,5 раз при $P_{присв} = 0{,}7$ снизить время обработки информационных пакетов по сравнению с алгоритмом WF2Q. В остальных случаях обработки информационных пакетов $r_2 = \overline{2, J}$ и $r_3 = \overline{J+1, R}$ уровней приоритетности эффективность разработанного алгоритма соизмерима с эффективностью известного $WF^2Q$.

Таким образом, приведенные результаты исследований позволили сделать вывод о эффективности разработанного метода управления доступом

к облачным телекоммуникационным ресурсам и возможности уменьшения времени обработки информационных пакетов первого уровня приоритетности до 4 раз в случае императивного администрирования и до 2 раз в случае справедливого распределения.

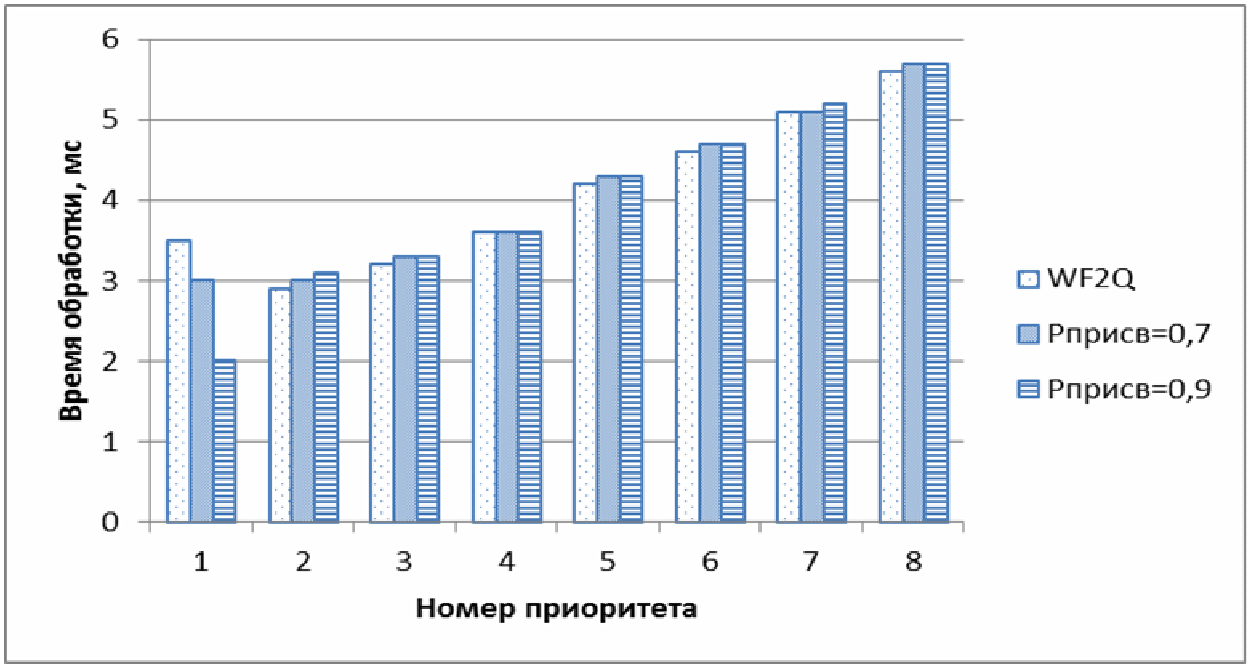



Рис. 4.3. Гистограммы исследования показателя времени обработки информационных пакетов различного уровня приоритетности в условиях справедливого распределения

## 4.4. Обоснование достоверности результатов математического моделирования

Для обоснования достоверности полученных во 2 и 3 разделах результатов проведено имитационное моделирование процесса обработки информационных пакетов в интеллектуальных узлах коммутации ТКС, в соответствии с условиями :

– все процессоры в подсистемы управления и обслуживания в узле связи однотипны и осуществляют обслуживание независимо друг от друга;

– один процессор может обслуживать в единицу времени такое количество пакетов, которое соответствует количеству пакетов, хранящихся в одной ячейке памяти буфера;

– длина информационного пакета $\ell_p$ = 1024 бита;

– число экспериментов $N$*=100.

По результатам имитационного моделирования для различного рода информации получены гистограммы времени обработки информационных пакетов в интеллектуальных узлах коммутации [56].

На рис. 4.4 представлены гистограммы времени обработки информационных пакетов метаданных $r_1$ уровня приоритетности (рис. 4.4. а), информационных пакетов протокола *SKYPE* $r_2$ – уровня приоритетности (рис. 4.4. б) и информационных пакетов *FTP(HTTP)*-трафика $r_3$ уровня приоритетности (рис. 4.4. в).

Выдвинутая гипотеза о нормальном распределении этой случайной величины была проверена по критерию согласия $\chi^2$ Пирсона [9]

$$\chi^2 = N^* \sum_{i=1}^{k} (P_i^* - P_i)^2 / P_i ,$$

где

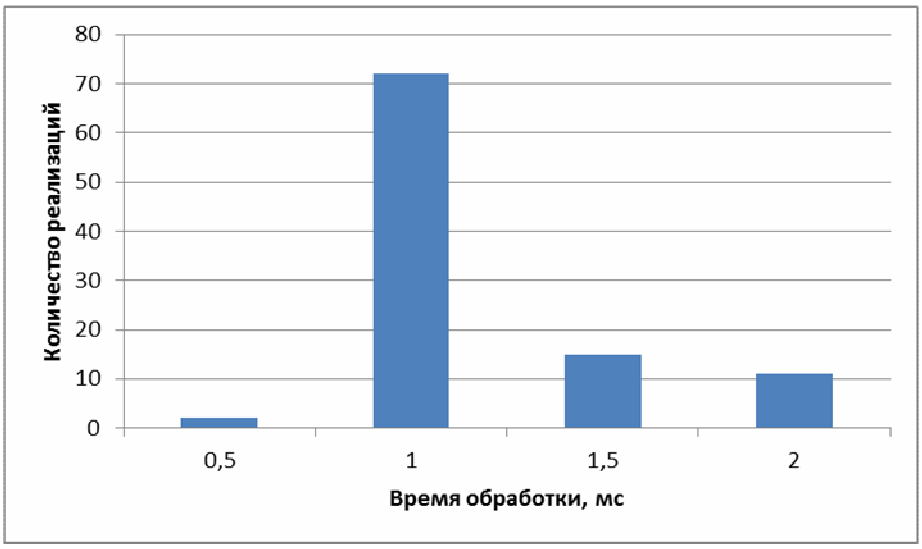
$k$ – число разрядов (интервалов) статистического ряда;

$P_i^*$ и $P_i$ – «статистическая» и теоретическая вероятности «попадания» заданного показателя в $i$-й разряд.

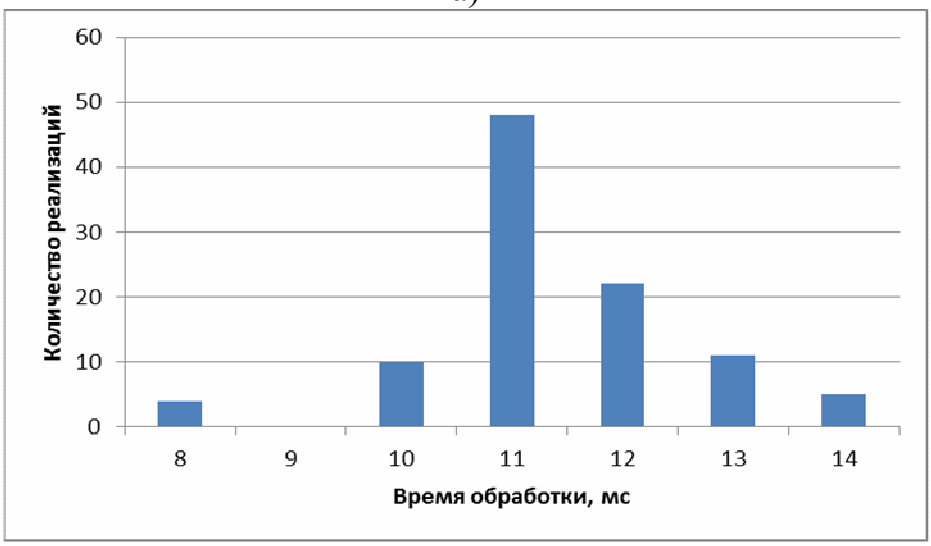
Проведенная проверка доказала правдоподобность гипотезы о том, что величина времени обработки информационных пакетов в интеллектуальном узле коммутации распределена по нормальному закону.

Получены оценки $t_{обр}^{(i)}$ математического ожидания и $D_{t_{обр}^{(i)}}$ дисперсии ($\sigma_{t_{обр}^{(i)}}$ среднеквадратического отклонения) случайной величины

$t_{обр}^{(i)}$ времени обработки информационных пакетов в интеллектуальном узле коммутации [56]




а)




б)


в)

Рис. 4.4. Гистограммы времени обработки информационных пакетов в интеллектуальном узле коммутации

$$\bar{t}_{обр}^{(i)} = \frac{\sum_{i=1}^{k} t_{обр}^{(i)}}{N^*}; \quad D_{\bar{t}_{обр}^{(i)}} = \frac{\sum_{i=1}^{k}\left(\bar{t}_{обр}^{(i)} - t_{обр}^{(i)}\right)^2}{N^* - 1}; \quad \sigma_{\bar{t}_{обр}^{(i)}} = \sqrt{D_{\bar{t}_{обр}^{(i)}}}.$$

Воспользовавшись известным выражением для расчета доверительной вероятности отклонения относительной частоты от постоянной вероятности в независимых испытаниях [9] определим доверительную вероятность того, что полученное в результате эксперимента значение времени обработки информационных пакетов «не отклониться» от математического ожидания $\bar{t}_{обр}^{(i)}$ более чем на 1:

$$P\left(\left|\bar{t}_{обр}^{(i)} - t_{обр}^{(i)}\right| < 1\right) = 2\Phi\left(1 \Big/ \sigma_{\bar{t}_{обр}^{(i)}}\right),$$

где Ф – функция Лапласа вида $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-t^2/2}\, dt$ [9].

Проведенное имитационное моделирование показало, что для всех исследуемых видов данных доверительная вероятность того, что значение статистической величины $t_{обр}^{(i)}$ «не отклониться» от математического ожидания $\bar{t}_{обр}^{(i)}$ более чем на 1 равно: $P \approx 0{,}97$.

По данным, полученным в разделе 3 и подразделе 4.3 (рис. 4.4.) в условиях императивного администрирования интеллектуального узла коммутации проведено сравнительное исследование результатов математического и имитационного моделирования. Результаты сравнения представлены на рис. 4.5. в виде графика плотности распределения времени $t_{обр}$ обработки информационных пакетов метаданных, при их передаче в «облачные» антивирусные системы, соответствующих им границ доверительного интервала:

$$I_\beta = \left[ \bar{J} - \varepsilon_\beta, \bar{J} + \varepsilon_\beta \right],$$

в которой истинное значение $\bar{J}$ попадает с доверительной вероятностью $\beta = 0{,}95$ и оценок его $\bar{t}_{обр}^{(i)}$ математического ожидания.

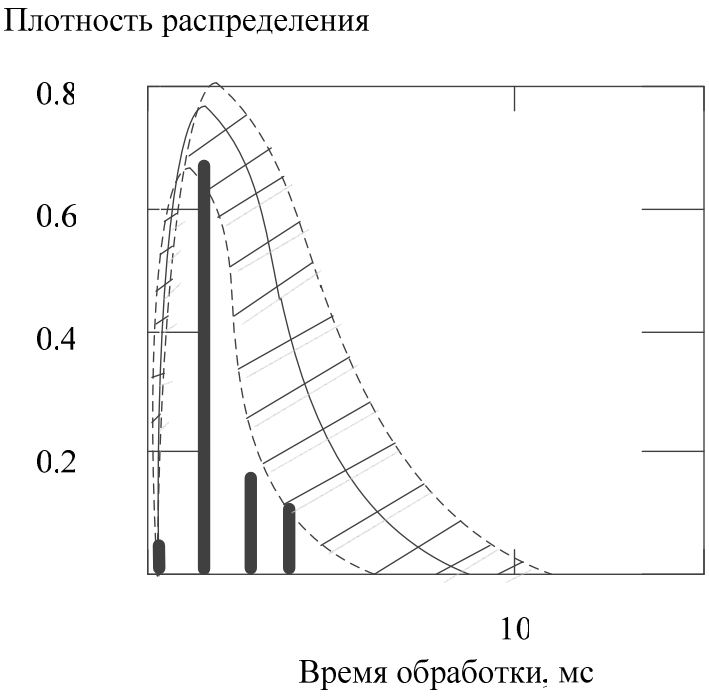



Рис. 4.5. График плотности распределения времени $t_{обр}$ обработки информационных пакетов, соответствующих им границ доверительного интервала и оценок его $\bar{t}_{обр}^{(i)}$ математического ожидания

Из графиков видно, что в ключевой тестовой ситуации (время обработки $t_{обр} \approx 1мс$) «расчетная» кривая $J$ (сплошная кривая), полученная в соответствии с разработанной в работе математической моделью (3.9), в большинстве практических случаев попадают в «усредненный» доверительный интервал (заштрихованная область).

Это подтверждает достоверность разработанной в 3 разделе математической модели узла коммутации с относительными приоритетами, резервированием ресурсов и учётом реальной надёжности обслуживающих

приборов и полученного в результате математического моделирования аналитического выражения для расчета времени обработки информационных пакетов в интеллектуальном узле коммутации.

## 4.5. Обоснование практических рекомендаций по использованию метода управления телекоммуникационными ресурсами для повышения оперативности передачи данных

Проведенный анализ современных интеллектуальных узлов коммутации (маршрутизаторов), поддерживающих усовершенствованные алгоритмы *QoS*, позволил выделить их основные функции:

– перераспределение информационных пакетов;

– подстройка параметров подключенной телекоммуникационной среды.

Практическая реализация этих функций возможна как на однопроцессорных узлах коммутации, так и на многопроцессорных. При этом важную роль играет операционная система, установленная на узлах коммутации. Так перераспределение информационных пакетов может осуществлять как отдельный интерфейсный процессор.

Проведенный анализ показал, что интеллектуальные узлы коммутации должны поддерживать различные алгоритмы управления – *CAR, WFQ, RRP, RSVP, DiffServ* и др. Для выполнения этих требования современные маршрутизаторы (например, *Cisco 3800 Series, Cisco 2800 Series, Cisco 7200 Series, 2210 Multiprotocol Routers, Motorola 6435/6455, ASUS RT-AC66U* и др.) добавляют протокол ресурсов, контрольный модуль и интерфейс к политике очередей уровня коммутации [56, 61].

В диссертационной работе предлагается дополнительную реализацию и использование в интеллектуальных узлах коммутации блоков управления телекоммуникационными ресурсами с учетом возможности приоритезации информационных пакетов (метаданных) для передачи в облачные антивирусные системы.

Несмотря на введение дополнительных механизмов регуляции и управления информационными пакетами современные узлы коммутации должны обеспечить максимальную скорость обслуживания информационных пакетов и других (более низких) уровней приоритетности. Сравнительный анализ современных телекоммуникационных технологий, методов управления сетевыми ресурсами, а также результаты проведенных в ходе диссертационной работы исследований позволили разработать практические рекомендации по повышению оперативности передачи метаданных в облачные антивирусные системы и применению разработанных моделей и метода, которые заключаются в следующем:

– для обеспечения качества обслуживания при передаче информационных пакетов $r_2 = \overline{2,J}$ уровня приоритета (в первую очередь мультимедийной информации) целесообразно объединение различных интерактивных служб и услуг в рамках единой многофункциональной информационной подсистемы;

– в процессе управления ТКС в целом и отдельными ее ресурсами необходимо проводить антивирусный мониторинг и оценку состояния узлов с помощью аппаратных или программных средств предотвращения и обнаружения вторжений (например, *Snort*);

– в процессе информационного обмена для повышения оперативности передачи метаданных в облачные антивирусные системы необходимо осуществлять целый комплекс мероприятий (адаптивное кодирование, статистическое мультиплексирование, адаптивная маршрутизация и др.) [27, 29];

– в системе управления очередями интеллектуального узла коммутации целесообразно использовать алгоритмы равномерного обслуживания очередей (*WFQ, WF*$^2$*Q*) с дополнительным внесением разработанных моделей, алгоритмов и методов, а также элементов первоочередного обслуживания информационных пакетов;

– в облачных антивирусных системах целесообразно использовать референсную архитектуру, основное назначение которой – адаптация оборудования к современным требованиям безопасности и повышение надежности используемых ресурсов [10-14].

При этом проведенные исследования показали, что одной из наиболее перспективных является облачная архитектура, базирующаяся на современных серверах семейства *Z* и в дополнение на нескольких серверах *HP* и *Sun(Oracle)*:

– управляющая машина *IBM z196* [68] (несколько CPU для поддержки *z/OS* и множество *IFL (Integrated Facility for Linux)* для поддержки *z/VM* и *zLinux*;

– *zBX*, управляемые из *z196* (поддерживают операционные системы *AIX*, *Linux, Windows*);

– *HP & SUN* (для поддержки *HP-UX* и *Solaris*);

– СУБД – *DB2* (все платформы), *Oracle* (все платформы), *MSSQL, Sybase* и другие системы управления базами данных;

– семейство программных продуктов *IBM Tivoli [*68].

Следует отметить, что постоянно растущий интерес к облачным технологиям требует от разработчиков новых конструктивных решений и практических рекомендаций. Последний пример таких рекомендаций распространен журналом *Infoworld* в рамках специального отчета *Cloud security, Deep Dive series, August 2011* под названием «Новая модель безопасности для новой эры» [84].

Авторы отчета настаивают на коренном пересмотре подхода к информационной безопасности при переходе к облачной среде. Это и повышенные требований к механизмам аутентификации, для которых необходимо усовершенствовать систему электронной цифровой подписи, и обеспечение доступности к облачным антивирусным ресурсам вне зависимости от их территориального (адресного) размещения. Кроме этого, в связи с появлением новых факторов, влияющих на состояние безопасности

ТКС, возникает необходимость пересмотра подходов к оценке уязвимости виртуальных соединений с облачными системами.

Таким образом, использование разработанных моделей и методов управления доступом к облачным телекоммуникационным ресурсам в условиях модернизации сетевого телекоммуникационного оборудования позволит повысить уровень информационной и функциональной безопасности как отдельных секторов так и ТКС в целом, при этом обеспечив заданный уровень качества обслуживания в процессе информационного обмена.

## Выводы по разделу 4

В разделе проведены исследования эффективности разработанного метода управления доступом к облачным телекоммуникационным ресурсам для обеспечения антивирусной защиты данных и обоснование практических рекомендаций по его использованию.

Определено, что в качестве показателя эффективности разработанного метода управления доступом к облачным телекоммуникационным ресурсам для обеспечения антивирусной защиты данных целесообразно выбрать время обслуживания информационных пакетов в интеллектуальных узлах коммутации.

Доказано, что использование разработанного метода до трех раз уменьшит время обслуживания информационных пакетов метаданных в интеллектуальных узлах коммутации при передаче их в облачные антивирусные системы. При этом будет обеспечен необходимый уровень качества обслуживания информационного обмена других телекоммуникационных услуг.

При оценке достоверности полученных в результате математического моделирования данных было проведено сравнение плотности распределения времени обработки информационных пакетов метаданных при их передаче в

«облачные» антивирусные системы и оценок его математического ожидания. Истинное значение выбранного показателя попадает в доверительный интервал с доверительной вероятностью $\beta = 0{,}95$

В качестве практических рекомендаций предложены технические новшества и решения, которые позволят повысить эффективность информационного обмена в современной ТКС.

Основные научные результаты, изложенные в третьем разделе, опубликованы в работах автора [38, 47, 48].

# ВЫВОДЫ

В диссертационной работе получено теоретическое обобщение и новое решение важной **научно-технической задачи**, состоящей в разработке метода управления телекоммуникационными ресурсами для повышения оперативности передачи данных.

Проведенные в диссертационной работе исследования, результаты решения научно-технической и частных научных задач, а также результаты расчетов и сравнительного анализа дали возможность получить следующие научные и практические результаты.

1. Анализ требований качества обслуживания и методов обеспечения показателей качества при передаче информационных потоков в телекоммуникационных системах, а также механизмов и средств службы поддержки качества обслуживания показал, что в условиях повышенного спроса на услуги Cloud-систем, используемые в настоящее время методы управления телекоммуникационными ресурсами не позволяют обеспечить оперативную передачу специальных сигнатур. Исследования основных методов и алгоритмов управления телекоммуникационными ресурсами позволили определить основные направления диссертационного исследования и сформулировать оптимизационную задачу минимизации времени передачи специализированных данных в облачные вычислительные системы.

2. Разработан метод априорной оценки требований оперативности передачи данных в условиях воздействия компьютерных вирусов, в основу которого положены математическая модель технологии распространения злоумышленного программного обеспечения в информационно-телекоммуникационных сетях и математическая GERT-модель технологии передачи метаданных в «облачные» антивирусные системы.

3. Разработана математическая GERT-модель технологии передачи метаданных в облачные антивирусные системы, которая отличается от

известных учетом показателей реальной надежности и особенностей многопутевой маршрутизации в соответствии с протоколами ($K$+4) уровня стратификации. Проведенное моделирование позволило определить, что максимальные значения плотности распределения времени формирования и передачи специальных сигнатур приходится на промежуток от 1 до 3 с. Использование полученных вероятностно-временных показателей позволило повысить точность оценки времени распространения злоумышленного программного обеспечения до 1,4 раза.

4. Разработана структурно-логическая GERT-модель технологии распространения компьютерных вирусов. Это позволило определить эквивалентную $W$-функцию времени распространения в ТКС наиболее опасных компьютерных вирусов типа *Flame* с конечными результатами лечения и иммунизации узлов ТКС, а также учесть фактор выхода из строя телекоммуникационных узлов.

5. Разработана математическая модель технологии распространения злоумышленного программного обеспечения в ТКС, в отличие от известных, учитывающую ключевую информацию о состояниях телекоммуникационных узлов в процессе деструктивных воздействий компьютерных вирусов, а также фактор использования облачного антивирусного обеспечения в процессе лечения, что позволило определить время распространения злоумышленного программного обеспечения в ТКС в условиях появления новых сценариев их деструктивного воздействия. Использование разработанного специального программного и математического обеспечения для моделирования технологии распространения злоумышленного программного обеспечения в ТКС позволило расширить спектр возможных сценариев их деструктивного воздействия до 30% и сформировать требования к вероятностно-временным показателям локализации и лечения узлов ТКС.

6. Разработан метод управления доступом в интеллектуальных узлах коммутации включающий в себя математическую модель интеллектуального

узла коммутации с обслуживанием информационных пакетов различного приоритета и усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам. Отличительной особенностью метода является комплексное использование стандартных критериев управления информационными потоками в интеллектуальных узлах коммутации с дополнительными, учитывающими возможность обслуживания информационных пакетов метаданных при их передаче в «облачные» антивирусные системы. Это позволило до 3 раз уменьшить время обслуживания информационных пакетов метаданных в интеллектуальных узлах коммутации при передаче их в облачные антивирусные системы.

7. Разработаны практические рекомендации по применению разработанного метода управления телекоммуникационными ресурсами, позволяющие адаптировать приведенные в диссертационной работе разработки к условиям и возможностям функционирования современных ТКС.

Результаты диссертационной работы внедрены в виде алгоритмов и средств для решения задач повышения оперативности передачи специализированных данных в облачные вычислительные системы:

– при проектировании системы управления телекоммуникационными ресурсами для повышения оперативности передачи данных, которые передаются по каналам связи интернет-сервис провайдера ООО «ИСП Империал», акт внедрения от 17.04.2015 г.;

– в учебном процессе Кировоградского национального технического университета, акт внедрения от 20.05.2015 г.

Использование результатов диссертационной работы подтверждено соответствующими актами внедрения (приложение Б).

Достоверность результатов диссертационного исследования подтверждается сходимостью результатов экспериментальных исследований, полученных при имитационном моделировании системы управления

доступом к облачным телекоммуникационным ресурсам с теоретическими и практическими результатами, отраженными в публикациях, и обусловлена их соответствием положениям известных теорий телетрафика, массового обслуживания, а также GERT-сетей.

Научное использование результатов, полученных в диссертационной работе, возможно в рамках последующего развития научного направления, которое связано с разработкой моделей и методов управления доступом к облачным телекоммуникационным ресурсам.

Практическое использование методов и средств, предложенных в диссертационной работе, возможно при разработке и модификации протоколов управления доступом к облачным телекоммуникационным ресурсам.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ


1. *Арипов М.Н.* Проектирование и техническая эксплуатация сетей передачи дискретных сообщений / М.Н. Арипов, Г.П. Захаров, С.Т. Малиновский, Г.Г. Яновский. М Радио и связь. 1988г. 360с
2. *Бабанин Д.В.* Модели распространения компьютерных вирусов на основе цепей Маркова / Д.В. Бабанин // Математическое и программное обеспечение вычислительных систем: межвуз. сб. науч. тр. / под ред. А.Н. Пылькина – М.: Горячая линия – Телеком, 2009. 156 с. – С. 89-93.
3. *Бабанин Д.В.* Оценка структурной защищенности компьютерной сети от вирусных атак / Д.В. Бабанин // Математическое и программное обеспечение вычислительных систем: межвуз. сб. науч. тр. / Под ред. А.Н. Пылькина – Рязань: РГРТУ, 2011.224 с. – С. 133-138.
4. *Бертсекас Д.* Сети передачи данных: пер. с англ. / Д. Бертсекас, Р. Галлагер; под ред. Б.С. Цыбакова. – М.: Мир, 1989. – 544 с.
5. *Вегешна Ш.* Качество обслуживания в сетях IP / Ш. Вегешна. М.:– Вільямс, 2003. – 368 с.
6. *Вишневский В.М.* Широкополосные беспроводные сети передачи информации / В.М. Вишневский, А.И. Ляхов, С.Л. Портной, И.В. Шахнович. – М.: Техносфера, 2005. – 591 с.
7. *Вишневский В.М.* Теоретические основы проектирования компьютерных сетей / В.М. Вишневский. – М.: Техносфера, 2003. – 512 с.
8. *Галкин В.А.* Телекоммуникации и сети / В.А. Галкин, Ю.А.Григорьев. – М.: МГТУ имени Н.Э. Баумана, 2003. – 608 с.
9. *Гмурман В.Е.* Теория вероятностей и математическая статистика / Владимир Ефимович Гмурман. – М.: Высшая школа, 2003. – 479 с.

10. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология Методы и средства обеспечения безопасности Часть 1 Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий [Електронний ресурс]. – Режим доступу до ресурсу: http://www.rfcmd.ru/sphider/docs/InfoSec/GOST-R_ISO_IEC_13335-1-2006.htm
11. ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции [Електронний ресурс]. – Режим доступу до ресурсу: http://protect.gost.ru/document.aspx?control=7&id=179072
12. *ДСТУ* 2481 – 94 Системи оброблення інформації інтелектуальні інформаційні технології. Терміни та визначення. – Х.: ДЕРЖСТАНДАРТ УКРАЇНИ, 1994. – 33 с.
13. *ДСТУ* В 3265 – 95. Зв'язок військовий. Терміни та визначення. – К.:УкрНДІССІ, 1995. – 23 с.
14. *ДСТУ ISO 9000:2007* Системи управління якістю. Основні положення та словник термінів [Електронний ресурс]. – Режим доступу до ресурсу: http://document.ua/docs/tdoc14237.php
15. *Дымарский Я.С.* Управление сетями связи: Принципы, протоколы, прикладные задачи / Я.С. Дымарский, Н.П. Крутякова, Г.Г. Яновский. – М.: ИТЦ «Мобильные коммуникации», 2003. – 384 с.
16. *Ершов В.А.* Мультисервисные телекоммуникационные сети / В.А. Ершов, Н.А. Кузнецов – М.: Изд. МГТУ им. Н.Э. Баумана, 2003. – 432 с.
17. *Зайченко Ю.П.* Компьютерные сети / Ю.П. Зайченко. – К.: Слово, 2003. – 256 с.
18. *Касперский Е.* Компьютерное зловредство / Е. Касперский. – СПб.: Питер, 2007. – 208 с.

19. *Касперский К.* Техника сетевых атак. [Електронний ресурс]. – Режим доступу до ресурсу: http://rghost.ru/download/43730077/8e48b6263ce45c7dc2a65a7453383dc33b22486d/Крис%20Касперски%20-%20Техника%20сетевых%20атак.pdf
20. *Касперский К.* Техника и философия хакерских атак. / К. Касперский. – М.: Солон-Пресс, 2004 – 272 с.
21. *Касперский К.* Записки исследователя компьютерных вирусов. / К. Касперский. – СПб.: Питер, 2006. – 316 с.
22. *Касперский К.* Компьютерные вирусы изнутри и снаружи. / К. Касперский. – СПб.: Питер, 2006. – 526 с.
23. *Кингман Дж.* Пуассоновские процессы / Дж. Кингман М.:МЦНМО, 2007. – 136 с.
24. *Клейнрок Л.* Вычислительные системы с очередями / Л. Клейнрок – М.:Мир, 1979. – 600 с.
25. *Кормен Т.* Алгоритмы: построение и анализ / Томас Кормен, Чарльз Лейзерсон, Рональд Ривест, Клиффорд Штайн. – М.:"Вильямс", 2005. –1296 с.
26. *Конахович Г.Ф.* Сети передачи пакетных данных / Г.Ф. Конахович, В.М.Чуприн. – К.:МК-Пресс, 2006. – 272 с.
27. *Королев А.В.* Адаптивная маршрутизация в корпоративных сетях / А.В. Королев, Г.А. Кучук, А.А. Пашнев. – Х.: ХВУ, 2003. – 224 с.
28. *Кучерявый Е.А.* Управление трафиком и качество обслуживания в сети Интернет / Евгений Андреевич Кучерявый. – СПб.: Наука и техника, 2004. – 336 с.
29. *Кучук Г.А.* Управление ресурсами инфотелекоммуникаций / Г.А. Кучук, Р.П. Гахов, А.А. Пашнев. – М.: Физматлит, 2006. – 220 с.
30. *Лагутин В.С., Степанов С.Н.* Телетрафик мультисервисных сетей связи / В.С. Лагутин, С.Н. Степанов. – М.: Радио и связь, 2000. – 320 с.

31. *Майника Э.* Алгоритмы оптимизации на сетях и графах: пер. с англ. / Э. Майника; под ред. Е.К. Масловского. – М.: Мир, 1981. – 321 с.
32. *Мохамад Гани Абу Таам* Разработка математической GERT-модели технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / А.А.Смирнов, Мохамад Гани Абу Таам // Информационные системы в управлении, образовании, промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – 498 с.
33. *Мохамад Гани Абу Таам* Метод управления доступом в интеллектуальных узлах коммутации / Мохамад Гани Абу Таам, А.А.Смирнов // Информационные технологии и защита информации в информационно-коммуникационных системах: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2015. – 486 с.
34. *Мохамад Гани Абу Таам* Математическая GERT-модель технологии передачи метаданных в облачные антивирусные системы / В.В.Босько, А.А.Смирнов, И.А.Березюк, Мохамад Гани Абу Таам // Збірник наукових праць "Системи обробки інформації". – Випуск 1(117). – Х.: ХУПС – 2014. – С. 137-141.
35. *Мохамад Гани Абу Таам* Структурно-логическая GERT-модель технологии распространения компьютерных вирусов / А.А.Смирнов, И.А.Березюк, Мохамад Гани Абу Таам // Системи управління, навігації та зв’язку. – Випуск 1(29). – П.: ПНТУ. – 2014. – С. 120-125.
36. *Мохамад Гани Абу Таам* Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Гани Абу Таам, А.А. Смирнов, А.В. Коваленко, С.А. Смирнов // Збірник наукових праць "Системи обробки інформації". – Випуск 9(125). – Х.: ХУПС – 2014. – С. 105-110.

37. *Мохамад Гани Абу Таам* Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Гани Абу Таам, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. Випуск 4 (41). – Харків: ХУПС. – 2014. – С. 48-52.
38. *Мохамад Гани Абу Таам* Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Гани Абу Таам, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 4(17). – Харків: ХУПС. – 2014. – С.90-95.
39. *Мохамад Гани Абу Таам* Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Гани Абу Таам, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Збірник наукових праць "Системи обробки інформації". – Випуск 1(126). – Х.: ХУПС – 2015. – С. 150-153.
40. *Мохамад Гани Абу Таам* Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты данных / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Системи озброєння і військова техніка. – Випуск 3(43) – Х.: ХУПС – 2015. – С. 100-107.
41. *Мохамад Гани Абу Таам* Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 3(19). – Х.: ХУПС. – 2015. – С. 134-141.

42. *Mohamad Abou Taam* Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.

43. *Мохамад Гани Абу Таам* GERT-модель технологии передачи данных в облачные антивирусные системы / А.А. Смирнов, В.В. Босько, Мохамад Гани Абу Таам // Збірник тез доповідей науково-практичної конференції «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку». м. Харків. 12-13 березня 2014 р. – Харків. АВВ МВС. – 2014. – С. 18-19.

44. *Мохамад Гани Абу Таам* Математическое моделирование технологии передачи сигнатур в облачные антивирусные системы / Мохамад Гани Абу Таам, А.А. Смирнов // Збірник тез VI міжнародної науково-практичної конференції “Проблеми і перспективи розвитку ІТ-індустрії”. м. Харків. 17-18 квітня 2014 р. – Харків: ХНЕУ. – 2014. – С. 260.

45. *Мохамад Гани Абу Таам* Анализ требований к качеству обслуживания в информационно-телекоммуникационных системах / А.А. Смирнов, Мохамад Гани Абу Таам // Збірник тез XVI міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування». м. Кіровоград. 11-12 квітня 2014 р. – Кіровоград: КНТУ. – 2014. – С. 124-126.

46. *Мохамад Гані Абу Таам* Дослідження та реалізація GERT-моделі технології розповсюдження комп’ютерних вірусів для захисту телекомунікаційних систем / Мохамад Гані Абу Таам, С.А. Смирнов // Збірник тез науково-практичної конференції «Інформаційні технології та комп’ютерна інженерія». м. Кіровоград. 4 грудня 2014 р. – Кіровоград: КНТУ. – 2014. – С. 168.

47. *Мохамад Гани Абу Таам* Исследование математических моделей технологии распространения компьютерных вирусов / А.А. Смирнов, Мохамад Гани Абу Таам, С.А. Смирнов // Збірник наукових праць міжнародної науково-практичної конференції «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації». м. Київ. 25-28 лютого 2015 р. – Київ: Європейський університет. – 2015. – С. 90-91.
48. *Мохамад Гани Абу Таам* Метод управления доступом к «облачным» ресурсам для защиты телекоммуникационных систем / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Збірник тез всеукраїнської науково-практичної конференції «Інформаційна безпека держави, суспільства та особистості». м. Кіровоград. 16 квітня 2015. – Кіровоград: КНТУ. – 2015. – С. 50-52.
49. *Мохамад Гани Абу Таам* Разработка метода управления доступом в интеллектуальных узлах коммутации / А.А. Смирнов, Мохамад Гани Абу Таам, С.А. Смирнов // Збірник тез VII міжнародної науково-практичної конференції “Проблеми і перспективи розвитку ІТ-індустрії”. м. Харків. 17-18 квітня 2015 р. – Харків: ХНЕУ. – 2015. – С. 14.
50. *Мохамад Гани Абу Таам* Реализация метода управления доступом в интеллектуальных узлах коммутации / А.А. Смирнов, Мохамад Гани Абу Таам // Збірник тез XVII міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування». м. Кіровоград. 17-18 квітня 2015 р. – Кіровоград: КНТУ. – 2015. – С. 91-92.
51. *Мохамад Гани Абу Таам* Реализация математической модели интеллектуального узла коммутации для обеспечения защищенности телекоммуникационной сети / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Збірник тез II Міжнародної науково-практичної Інтернет-конференції «Інформаційна та економічна безпека» (INFECO-2015)». м. Харків. 21-22 травня 2015 р. – Харків: ХІБС УБС НБУ. – 2015. – С. 20-24.

52. *Мохамад Гани Абу Таам* Разработка математической модели технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Сборник тезисов XI международной конференции "Стратегия качества в промышленности и образовании". г. Варна. Болгария. 01 – 06 июня 2015 г – Варна. ТУВ. – 2015. – С. 488-491
53. *Мохамад Гани Абу Таам* Метод управления доступом к облачным телекоммуникационным ресурсам для обеспечения защиты данных / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Збірник тез Міжнародної науково-практичної конференції «Комп'ютерні технології та інформаційна безпека». м. Кіровоград. 2-3 липня 2015 р. – Кіровоград: КНТУ. – 2015. – С. 4-5.
54. *Мохамад Гани Абу Таам* Имитационная модель системы управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Збірник тез першої всеукраїнської науково-практичної конференції «Перспективні напрями захисту інформації». м. Затока. 7-9 вересня 2015 р. – Одеса: ОНАЗ. – 2015. – С. 90-94.
55. МСЭ-Т Рекомендация G.101. Международные телефонные соединения и цепи – Общие определения //11/2003. [Електронний ресурс]. – Режим доступу до ресурсу: http://www. telecom61.ru›SharedFiles/Download.aspx? …pageid=106
56. *Одом Ш.* Коммутаторы CISCO / Ш. Одом, Х. Ноттингем – М.:"Кудиц-Образ", 2003. – 528 с.
57. *Олифер В.Г.* Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В.Г. Олифер, Н.А. Олифер. –2-е изд. – СПб.: Питер, 2007. – 958 с.
58. *Руководство* по технологиям объединенных сетей. 4-е изд. / пер.с англ. и ред. А.Н. Крикуна – М.: Изд. дом «Вильямс», 2005. – 1040 с.

59. *Свами М.Н., Тхуласираман К.* Графы, сети и алгоритмы: пер. с англ. / М.Н. Свами, К. Тхуласираман; под ред. В.А. Горбатова. – М.: Мир, 1984. – 454 с.
60. *Семенов С.Г.* Анализ методов прогнозирования в телекоммуникационных сетях автоматизированных систем управления / С.Г.Семенов // Збірник наукових праць «Системи управління, навігації та зв'язку», – К.:ЦНДІ навігації і управління, – 2008.-Вип. 2(6) .- С.134-137
61. *Семенов С.Г.* Математическая модель процесса доставки информационных пакетов в компьютерной сети системы критического применения / С.Г.Семенов, И.В.Ильина // Науково-технічний журнал «Радіоелектронні і комп'ютерні системи» Х.:ХАІ, – 2008.-Вип. 1(28) – С.162-165
62. *Семенов С.Г.* Оптимизация трафика на основе сбалансированной загрузки информационно-телекоммуникационной сети // Системи обробки інформації. – Х.: ХВУ, 2004. – № 8(36). – С.206-210
63. *Семенов С.Г.* Математическая модель мультисервисного канала связи на основе экспоненциальной GERT-сети / С.Г. Семенов, Є.В. Мелешко, Я.В. Ілюшко // Системи озброєння і військова техніка. – Х.:ХУ ПС. – 2011. – Вип. 3(27). – С. 64-67.
64. *Семенов С.Г.* Математична модель системи криптографічного захисту електронних повідомлень на основі GERT-мережі / С.Г. Семенов, О.О. Сур // Системи управління, навігації та зв'язку. – К.:ЦНДІ навігації і управління. – 2012. – Том 1. Вип. 1(21). – С. 131-137
65. *Семенов С.Г.* Исследования вероятностно-временных характеристик мультисервисного канала связи с использованием математического аппарата GERT-сети / С.Г. Семенов, В.В. Босько, І.А. Березюк // Системи обробки інформації. – Х.: ХУ ПС. – 2012. – Том 1. Вип. 3(101). – С. 139-142.

66. *Семенов С.Г.* Моделирование защищенного канала связи с использованием экспоненциальной GERT-сети / С.Г. Семенов, А.А. Можаев // Информатика, математическое моделирование, экономика. – Смоленськ.: Смоленский филиал АНО ВПО ЦС РФ "Российский университет кооперации". – 2012. – Том.1. – С. 152-160.

67. *Семенов С.Г.* Методика математического моделирования защищенной ИТС на основе многослойной GERT-сети / С.Г. Семенов // Вісник Національного технічного університету «Харківський політехнічний інститут». – Х.:НТУ «ХПІ». – 2012. –№62 (968). – С 173-181.

68. *Семенов С.Г.* Защита данных в компьютеризированных управляющих системах / С.Г. Семенов, В.В. Давыдов, С.Ю. Гавриленко. – LAP Lambert Academic Publishing GmbH & Co. KG (Саарбрюккен, Германия), 2014. – 236 с.

69. *Смирнов А.А.* Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.

70. *Смирнов А.А.* Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.

71. *Современные* телекоммуникации. Технологии и экономика / [В.Л. Банкет, О.В. Бондаренко, П.П. Воробьенко и др.]; под ред. С.А. Довгого. – М.: Эко-Трендз, 2003. – 320 с.

72. *Столлингс В.* Современные компьютерные сети / Вильям Столлингс.– СПб.: Питер, 2003. – 778 с.

73. *Таненбаум Э.* Компьютерные сети / Эндрю Таненбаум; пер. с англ. А. Леонтьев. – СПб.: Питер, 2002. – 848 с.

74. *Телекоммуникационные* системы и сети*:* учебное пособие. В 3 томах / [В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославцев]; под ред. В.П. Шувалова. – М.: Горячая линия-Телеком, 2005, т. 3 – 592 с.

75. *Уолрэнд Дж.* Телекоммуникационные и компьютерные сети / Дж. Уолрэнд. – М.: Постмаркет, 2001. – 480 с.

76. *Хайкин С.* Нейронные сети: полный курс / С. Хайкин. – М.:Вильямс, 2006. – 1103 с.

77. *Шелухин О.И.* Фрактальные процессы в телекоммуникациях: моногр. / О.И. Шелухин, А.М. Тенякшев, А.В. Осин – М.: Радиотехника, 2003. – 480 с.

78. *A. Elwalid* Routing and Protection in GMPLS Networks: From Shortest Paths to Optimized Designs / A. Elwalid, D. Mitra, I. Saniee, and I. Widjaja. //Journal of lightwave technology. – 2003. – №21(11), P. 2828-28-38.

79. *A.B. Bagula* Online Traffic Engineering: The Least Interference Optimization Algorithm / A.B. Bagula, M. Botha, and A.E Krzesinski. // IEEE Communications Society – 2004, P. 1232-1236.

80. *Anees. Shaikh* Evaluating the Impact of Stale Link State on Quality-of-Service Routing / Anees Shaikh, Jennifer Rexford, and Kang G. Shin. // IEEE/ACM Transactions on Networking. – 2001. – №9(2), P. 162-176.

81. *Chakraborty Basabi* Simultaneous Search for Multiple Routes using Genetic Algorithm / Basabi Chakraborty // IEEE lntemational Conference on Computational oltelligencs for Measurement System and Applications Boston. MA, USA, 14-16, July 2004, P. 77-80/

82. *C. Barakat* On TCP performance in a heterogeneous network: a survey / C. Barakat, E. Altman, and W. Dabbous. // IEEE Communications Magazine. – 2000. – №38(1). – P. 40 – 46.

83. *C. Casetti* A New Class of QoS Routing Strategies Based on Network Graph Reduction / C. Casetti, R. Lo Cigno, M. Mellia, M. Munafo.// Proceedings of IEEE INFOCOM. – 2002, P.715-722.

84. *Cloud security, Deep Dive series, August 2011 [*Электронный ресурс]. – Режим доступа к ресурсу: http://www.slideshare.net/kimrenejensen/cloud-security-deep-dive-2011#14375029197881&fbinitialized

85. *Chris Loeser* Distributed Path Selection (DPS) a Traffic Engineering Protocol for IP-Networks / Chris Loeser, Andre Brinkmann, Ulrich Ruckert. // Proceedings of the 37th Hawaii International Conference on System Sciences – 2004, P. 1-8.

86. *Dai Boong.* Dynamic Class Selecting Mechanism for Guaranteed Service with Minimum Cost over Relative Differentiated-Services Networks / Dai Boong Lee, Hwangjun Song. // IEEE International Conference on Multimedia and Expo (ICME) – 2004, P. 237-240.

87. *Gang Cheng.* A New Heuristics For Finding The Delay Constrained Least Cost Path / Gang Cheng, Nirwan Ansari. // IEEE GLOBECOM – 2003, P. 3711-3715.

88. *Gang Cheng.* A New Deterministic Traffic Model for Core-Stateless Scheduling / Gang Cheng, Li Zhu, and Nirwan Ansari // IEEE Transactions on communications. – 2006. – № 4, P. 704-713.

89. *Hui Ma* A Model and Methodology for Composition QoS Analysis of Embedded Systems / Hui Ma, Dongfeng Wang, Farokh Bastani, I-Ling Yen, Kendra Cooper. // Proceedings of the 11th IEEE Real Time and Embedded Technology and Applications Symposium (RTAS'05) – 2005, P. 1-10.

90. *H. Chaskar* Considerations from the Service Management Research Group (SMRG) on Quality of Service (QoS) in the IP Network / H. Chaskar M. Eder, S. Nag // RFC-3387. September 2002

91. ITU-T Recommendations [Электронний ресурс]. – Режим доступа к ресурсу: http://www.itu.int/ITU-T/recommendations/index.aspx?ser=Y

92. *Ji Li* A Two-Step Approach to Restorable Dynamic QoS Routing / Ji Li, Kwan L. Yeung. // IEEE Communications Society. – 2004, P. 1166-1170.

93. *Jianbin Wei* Feedback Control Approaches for Quality of Service Guarantees in Web Servers / Jianbin Wei, Cheng-Zhong Xu. // NAFIPS 2005. Annual Meeting of the North American Fuzzy Information Processing Society – 2005. P. 700-705

94. *Jiang Hu* A Timing-Constrained Simultaneous Global Routing Algorithm / Jiang Hu, Sachin S. Sapatnekar. // IEEE Transactions on computer-aided design of integrated circuits and systems. – 2002. – №21(9), P. 1025-1036.

95. *Jeffrey O* White, Directed-Graph Epidemiological Model of Computer Viruses / Jeffrey O. Kephart, Steve R. // IEEE Symposium on Security and Privacy, 1991. –P.343. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.research.ibm.com/antivirus/SciPapers/Kephart/VIRIEEE/ virieee.gopher.html

96. *Joao Luis Sobrinho.* Algebra and Algorithms for QoS Path Computation and Hop-by-Hop Routing in the Internet / Joao Luis Sobrinho. // IEEE/ACM Transactions on networking. – 2002. – №10(4), P. 541-55.

97. *Joo Young Hwang,* A Fast Path Planning by Path Graph Optimization / Joo Young Hwang, Jun Song Kim, Sang Seok Lim, and Kyu Ho Park. // IEEE Transactions on systems, man, and cybernetics-part a: systems and humans. – 2003. – №1, P. 121-128.

98. *Jui-Fa Chen* A Message Interchange Protocol based on Routing Information Protocol in a Virtual World / Jui-Fa Chen, Wei-Chuan Lin. // Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05) – 2005, P. 201-208.

99. *Jun Wang.* Hop-by-Hop Routing Algorithms For Premium-class Traffic In DiffServ Networks / Jun Wang, Klara Nahrstedt. // Proceedings of IEEE INFOCOM. – 2002, P. 705-714.

100. *K.Tsakalis* A new indirect adaptive schemes for time-varying plants / K.Tsakalis, P. Ionnou // IEEE Trans. Autom. Control. 1990. Vol. AC-35. № 6. – P. 697-705.

101. *K.S. Narendra* Stable adaptive schemes for system: identification and control / K.S. Narendra, B. Kudva // IEEE Trans. on Syst., Man and Cybern. 1974. Vol. SMC-4. № 6. – P. 542-560.

102. *Leland, W.* The Self-Similar Nature of Ethernet Traffic (Extended Version) / W. Leland, M. Taqqu, W. Willinger, D. Wilson // IEEE/ACM Transactions on Net-working, 1994.

103. *L. Ljung* System Identification – Theory for the User. / L.Ljung // Prentice Hall, Upper Saddle River, N. J. 2nd edition, 1999. – 499 p.
104. *Mohamed G. Gouda.* Maximizable Routing Metrics / Mohamed G. Gouda, Marco Schneider. // IEEE/ACM Transactions on networking. – 2003. – №11(4), P. 663-675.
105. *Murali Kodialam*. Online Multicast Routing With Bandwidth Guarantees: A New Approach Using Multicast Network Flow / Murali Kodialam, T. V. Lakshman, and Sudipta Sengupta. // IEEE/ACM Transactions on networking. – 2003. – №11(4), P. 676-686.
106. *Nianjun Zhou,* The Impact of Traffic Patterns on the Overhead of Reactive Routing Protocols / Nianjun Zhou, Huaming Wu, and Alhussein A. Abouzeid // IEEE Journal on selected areas in communications. – 2005. – №23(3), P. 547-560.
107. *Paolo Narvaez* New Dynamic Algorithms for Shortest Path Tree Computation / Paolo Narvaez, Kai-Yeung Siu, Hong-Yi Tzeng.// IEEE/ACM Transactions on Networking. – 2000. – №8(6), P. 734-746.
108. *Pritsker, A. A.* Modeling and analysis using Q-GERT networks / *Pritsker, A. A. //* New York: Wiley : Distributed by Halsted Press, 1979.
109. *Pritsker, A. A.* GERT: Graphical Evaluation and ReviewTechnique. Part I. Fundamentals / Pritsker, A. A., Happ W. W. // The Journal of Industrial Engineering (May 1966).
110. *P. Grassberger* Characterization of strange attractors, / P. Grassberger, I. Procaccia. // Phys. Rev. Lett. 58. . 1983. . P. 2387.2389.
111. *S. K. Lam* Accelerating The K-Shortest Paths Computation in Multimodal Transportation Networks / S. K. Lam and T. Srikanthan. // The IEEE 5th international conference on intelligent transportation system, 3-6 september 2002, Singapore, P. 491-495.
112. *S. Blake et al.,* "An Architecture for Differentiated Services," RFC 2475, Dec. 1998.

113. *Semenov S.G.* Mathematical Modelling of the Spreading of Software Threats in Computer Network / S.G. Semenov, V.V. Davydov, S.O. Engalichev // Proceedings of the XIth International Conference TCSET'2012 «Modern problems of radio engineering, telecommunications and computer science». – Lviv – Slavske, Ukraine 2012. – P. 329

114. *Semenov S.G.* A Mathematical Model for Technology for Spreading Malicious Software across Heterogeneous Networks based on Markov Chains / Semenov S., Davydov V.// European Researcher, 2014, Vol.(66), N1-1. – pp. 21-30.

115. *S. Nuyan,* Minimal order arbitrarily fast adaptive observer and identifies / S. Nuyan, R. L. Carrol // IEEE Trans. Automat. Control. 1979. Vol. AC-24. № 2. P. 496-499.

116. *Srihari Nelakuditi,.* On Localized Control in QoS Routing / Srihari Nelakuditi, Srivatsan Varadarajan, and Zhi-Li Zhang.// IEEE Transactions on Automatic Control. – 2002. – №47(6), P. 1026-1032.

117. *Stefan Soucek* Quality of Service Concerns in IP-Based Control Systems / Stefan Soucek, Member, Thilo Sauter, Member. // IEEE Transactions on industrial electronics. – 2004. – №51(6), P. 1249-1258.

118. *Sudha Krishnamurthy* An Adaptive Quality of Service Aware Middleware for Replicated Services / Sudha Krishnamurthy, William H. Sanders, Fellow, Michel Cukier // IEEE Transactions on parallel and distributed systems. – 2003. – №14(11), P. 1112-1125.

119. TL 9000 Quality Management System for Telecommunications [Электронний ресурс]. – Режим доступа к ресурсу: http://www.tuvam.com/services/qmservices/tl9000.cfm

120. *Vutukury S.* MDVA: A Distance-Vector Multipath Routing Protocol / Vutukury S., Garcia-Luna-Aceves J. J.// Proc. IEEE INFOCOM. – Anchorage, 2001. – P. 557-564.

121. *Vutukury S.* MPATH: a loop-free multipath routing algorithm / Vutukury S., Garcia-Luna-Aceves J. J.// Elsevier Journal of Microprocessors and Microsystems. – 2001. -24(6). – P. 319-327.

122. *Wendong Xiao* Evaluation of Heuristic Path Selection Algorithms' for Multi-Constrained QoS Routing / Wendong Xiao, Boon Hee Soong, Choi Look Law, Yong Liang Guan. // IEEE International Conference on Networking, Sensing & Control Taipei, Taiwan, March 21-23, 2004, P. 112-116.

123. *F. C. Schweppe* Uncertain dynamic system. New Jersey: Prentic- Hall Inc., Englewood Cliff, 1973. – 210 p.

124. *F. Takens* "Detecting strange attractors in turbulence in Dynamical Systems and Turbulence", Warwick, 1980, eds. D.Rang and L.S.Young, Lecture Notes in Mathematics, 1981, V. 898. P. 366-381.

125. *Xin Yuan* Heuristic Algorithms for Multi–Constrained Quality of Service Routing / Xin Yuan , Xingming Liu. // Proceedings of IEEE INFOCOM. – 2001, P. 844-853.

# Приложение А

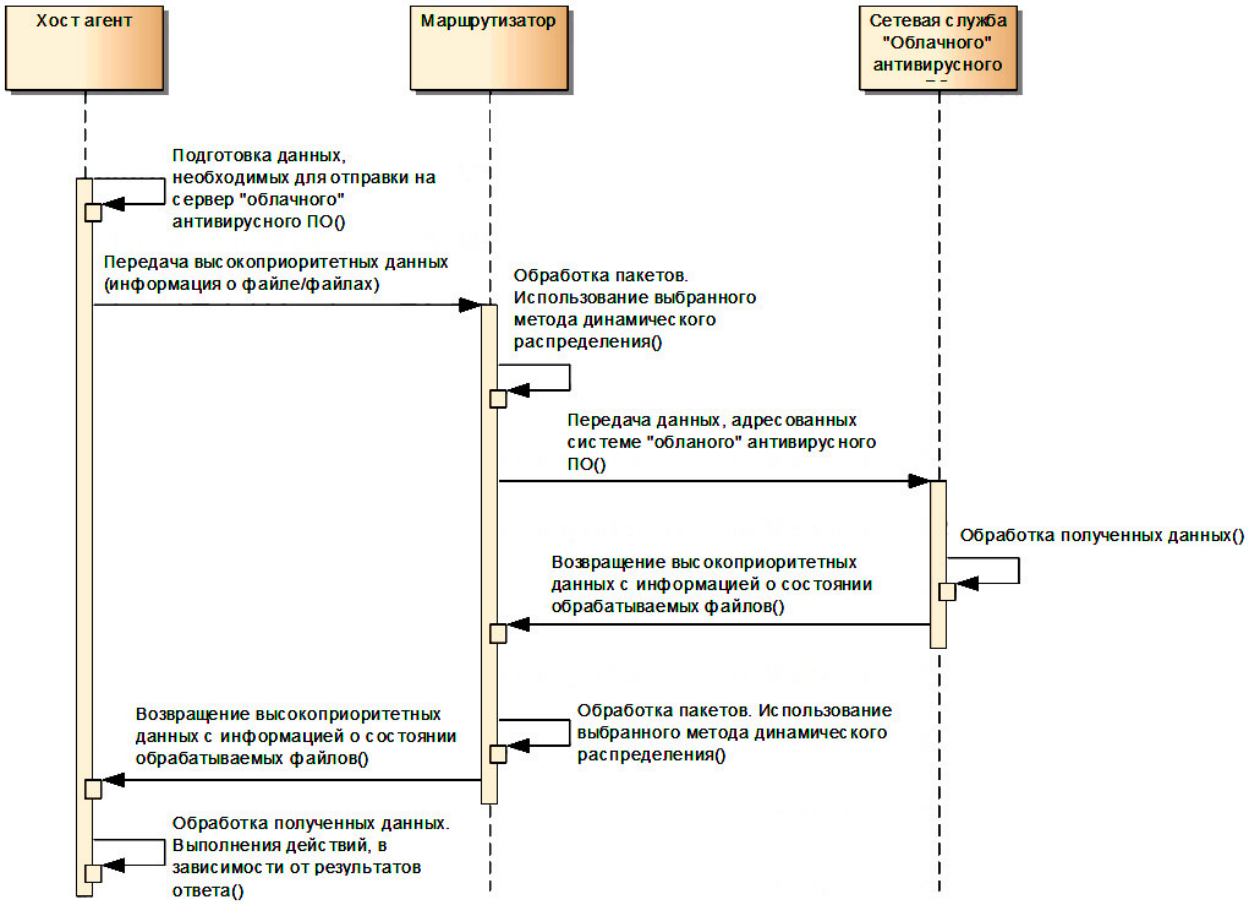



Рис. А.1. Диаграмма последовательностей процедур информационного обмена с облачными антивирусными системами

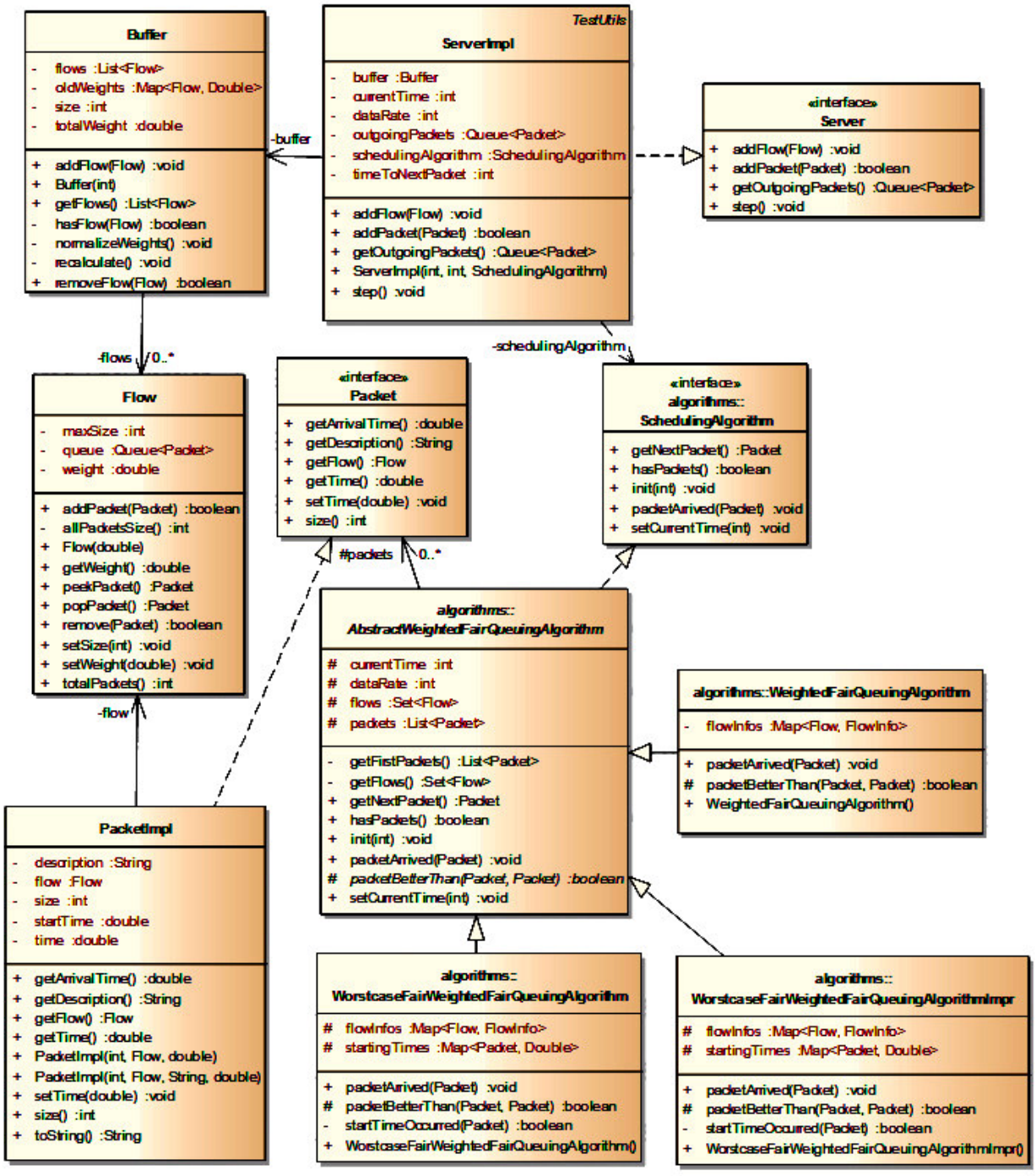



Рис. А.2. Диаграмма классов в разработанном программном комплексе

# Приложение Б

## Акты реализации результатов диссертационной работы

Imperial
Интернет сервис провайдер

ТОВ «ІМПЕРІАЛ-НЕТ»
тел: +38 (0522) 27-60-06
фкс : +38 (0522) 27-60-91
e-mail : office@imperial.net.ua
http://www.imperial.net.ua

ЗАТВЕРДЖУЮ:
Директор ТОВ «Імперіал Нет»
т.м. «ISP Imperial»

«14» квітня 2015 р.

АКТ
про впровадження результатів дисертаційної роботи
аспіранта кафедри «Програмування та захисту інформації»
Кіровоградського національного технічного університету
Мохамада Гані Абу Таам

Комісія у складі голови – Директора ТОВ «Імперіал Нет» Бур'янова К.В., членів комісії – провідного розробника ТОВ «Імперіал Нет» Король К.В., провідного розробника ТОВ «Імперіал Нет» Дуб О.В. склала цей акт про те, що у діяльності ТОВ «Імперіал Нет» реалізовано результати наукових досліджень Мохамада Гані Абу Таам: автоматизований програмний засіб управління чергами в інтелектуальному вузлі комутації, що дозволило до 3-х разів зменшити час обслуговування інформаційних пакетів метаданих в інтелектуальних вузлах комутації.

Голова комісії
Директор ТОВ «Імперіал Нет» _____ Бур'янов К.В.

Члени комісії:
провідний розробник _____ Король К.В.

провідний розробник _____ Дуб О.В.

ТОВ «ІМПЕРІАЛ-НЕТ»
вул. Єгорова 8
м. Кіровоград,
Україна, 25006

ПАТ КБ «ПриватБанк»
Р/Р : 26000052913562
МФО : 323583
ЄДРПОУ.: 39758019

тел : +38 (0522) 27-60-06
фак: +38 (0522) 27-60-91
office@imperial.net.ua
isp@imperial.net.ua
http://www.imperial.net.ua

ЗАТВЕРДЖУЮ:
Проректор з наукової роботи
Кіровоградського національного
технічного університету
_____ О.М. Левченко
«20» травня 2015 р.

АКТ

реалізації результатів наукових досліджень дисертаційної роботи аспіранта кафедри «Програмування та захисту інформації» Мохамада Гані Абу Таам

Комісія у складі голови – заступника завідуючого кафедрою «Програмування та захисту інформації» Кіровоградського національного технічного університету кандидата фізико-математичних наук, доцента Якименко Н.М., членів комісії – доцента кафедри «Програмування та захисту інформації» кандидата технічних наук, Мелешко Є.В., доцента кафедри «Програмування та захисту інформації» кандидата технічних наук, доцента Коваленко О.В. склала цей акт про те, що при розробці лекційних, практичних та лабораторних занять з навчальних дисциплін «Комп'ютерні мережі» та «Проектування й дослідження комп'ютерних мереж» у навчальному процесі Кіровоградського національного технічного університету були використані наступні результати наукових досліджень Мохамада Гані Абу Таам:

1. Метод управління доступом в інтелектуальних вузлах комутації, що відрізняється від відомих комплексним використанням стандартних критеріїв управління інформаційними потоками в інтелектуальних вузлах комутації з додатковими, які враховують можливість обслуговування інформаційних пакетів метаданих при їх передачі до хмарних обчислювальних систем, що дозволило підвищити оперативність обслуговування інформаційних пакетів метаданих в інтелектуальних вузлах комутації при їх передачі до хмарних обчислювальних систем.

2. Математична модель технології передачі метаданих у хмарні обчислювальні системи, яка відрізняється від відомих урахуванням показників реальної надійності та особливостей багатошляхової маршрутизації відповідно до протоколів мережевого рівня, що дозволило визначити функцію і щільність розподілу ймовірностей часу передачі метаданих у хмарні обчислювальні системи.

3. Математична модель технології розповсюдження зловмисного програмного забезпечення в ТКС, яка на відміну від відомих враховує ключову інформацію про стан телекомунікаційних вузлів в процесі деструктивних впливів комп'ютерних вірусів, а також фактор використання хмарного антивірусного забезпечення в процесі лікування, що дозволило визначити час

розповсюдження зловмисного програмного забезпечення в ТКС в умовах появи нових сценаріїв їхнього деструктивного впливу.

Застосування результатів дисертаційних досліджень Мохамада Гані Абу Таам дозволило підвищити рівень засвоєння навчального матеріалу з дисциплін «Комп'ютерні мережі» та «Проектування й дослідження комп'ютерних мереж» за рахунок більш поглибленого вивчення сучасних та перспективних методів передачі та перетворення інформації у телекомунікаційних мережах.

Голова комісії
Заступник завідуючого кафедри «Програмування та захисту інформації»
Кіровоградського національного
технічного університету
кандидат фізико-математичних наук, доцент Н.М. Якименко

Члени комісії:
доцент кафедри «Програмування та захисту інформації»
кандидат технічних наук, доцент Є.В. Мелешко

доцент кафедри «Програмування та захисту інформації»
кандидат технічних наук, доцент О.В. Коваленко