Книга 20

Оценка сетевых характеристик компьютерных сетей в условиях информационного вредоносного воздействия

Федеральное агентство по образованию
Государственное образовательное учреждение
высшего профессионального образования
Владимирский государственный университет

КОМЛЕКСНАЯ ЗАЩИТА
ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ.
КНИГА 20

Л.М.ГРУЗДЕВА Ю.М.МОНАХОВ, М.Ю.МОНАХОВ

ОЦЕНКА СЕТЕВЫХ ХАРАКТЕРИСТИК КОМПЬЮТЕРНЫХ СЕТЕЙ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ВРЕДОНОСНОГО ВОЗДЕЙСТВИЯ

Учебное пособие

Владимир 2010

УДК 930.1
ББК 32.81

Редактор серии доктор технических наук, профессор
М.Ю.Монахов
Рецензенты:
Кандидат технических наук, доцент
зав. кафедрой оперативно-технической деятельности
Владимирского юридического института ФСИН России
К.Н. Курысев
Доктор технических наук, профессор
Владимирского государственного университета
О.В.Веселов
Печатается по решению редакционно-издательского совета
Владимирского государственного университета

Груздева Л.М., Монахов Ю.М., Монахов М.Ю.
Оценка сетевых характеристик компьютерных сетей в условиях информационного вредоносного воздействия: учебное пособие. / Владим. гос. ун-т. – Владимир: Изд-во Владим. гос. ун-та, 2010. – с. (Комплексная защита объектов информатизации. Кн.20.)
ISBN

Представлен теоретический и практический материал по аналитическому и имитационному моделированию компьютерных сетей в условиях воздействия вредоносных и антивирусных программ, предложены модели и алгоритмы оценки сетевых характеристик. Предназначено для студентов специальности 090104 «Комплексная защита объектов информатизации».

Библиогр.: назв.

ББК 32.81

ISBN

Предисловие

Проектирование компьютерных сетей (КС) можно представить как решение последовательности проектных задач, которые включают задачи синтеза и задачи анализа системы и ее частей.

Любая задача синтеза состоит в том, чтобы построить из заданного множества элементов некоторую систему, обладающую заранее указанными свойствами. Задача анализа является обратной по отношению к задаче синтеза и состоит в выделении отдельных элементов заданной системы и установлении их параметров. При проектировании КС задача анализа КС рассматривается как задача проверки того, обладает ли построенная система заранее указанными свойствами. Решение задач анализа и синтеза КС и её частей осуществляется с помощью моделей проектируемой КС, в качестве которых используются описания, схемы, чертежи, математические модели и т.д.

Результаты решения задач анализа используются при решении задач синтеза, а результаты синтеза вновь подвергаются анализу. Модели КС развиваются, уточняются и на определённой стадии превращаются в проект КС, т.е. в совокупность документов, содержащих сведения, необходимые и достаточные для изготовления спроектированной КС в заданных условиях.

Задача анализа производительности КС является одной из важнейших среди задач проектирования КС. В общем виде задача анализа производительности КС состоит в том, чтобы оценить показатели производительности конкретной КС при заданных параметрах ее технического, программного обеспечения и внешней среды КС. К таким параметрам могут относиться быстродействия устройств, характеристики сложности программ, интенсивности потоков требований на выполнение программ, условия внешнего окружения (пропускная способность

арендуемых линий связи, наличие случайных и преднамеренных воздействий информационного и иного характера, приводящие к непредсказуемому функционирования КС), и другие.

Решая задачу анализа производительности, необходимо учитывать случайную природу многих факторов, от которых зависит производительность КС. Так, случайными часто являются моменты поступления в КС требований, объёмы подлежащей обработке информации, последовательность необходимых для ее обработки операций.

Сложность структуры КС и необходимость учёта случайных факторов делают задачу анализа производительности КС очень сложной. Поэтому все более широкое распространение для анализа производительности КС получает метод математического моделирования.

Моделирование - один из наиболее распространенных методов исследования процессов функционирования сложных систем. Известно достаточно большое количество методов построения математических моделей и средств реализации моделирующих алгоритмов. Наиболее распространенными из них являются системы и сети массового обслуживания.

В терминах систем массового обслуживания (СМО) описываются многие реальные системы: вычислительные системы, узлы сетей связи, системы посадки самолетов, магазины, производственные участки - любые системы, где возможны очереди и (или) отказы в обслуживании.

Усложнение структур и режимов реальных систем, особенно в условиях вредоносного информационного воздействия, затрудняет применение классических методов теории массового обслуживания ввиду возрастающей размерности решаемых задач. Одним из возможных путей преодоления размерности является использование моделей в форме сетей массового обслуживания (СеМО).

Теория массового обслуживания связана с разработкой и анализом математических, т.е. абстрактных, моделей, которые описывают процесс обслуживания некоторых объектов, поступающих на вход обслуживающего прибора в виде некоторого потока, и образующего в общем случае очередь на входе обслуживающего прибора.

Целью использования СМО как модели является анализ качества функционирования систем-оригиналов.

В свою очередь, СеМО используют для определения важнейших системных характеристик информационных систем: производительности; времени доставки пакетов; вероятности потери сообщений и блокировки в узлах; области допустимых значений нагрузки, при которых обеспечивается требуемое качество обслуживания и др.

В теории СеМО фундаментальным является понятие состояния сети. Важнейшая характеристика сетей МО - вероятности их состояний. Для определения вероятностей состояний СеМО исследуют протекающий в сети случайный процесс. В качестве моделей протекающих в СеМО процессов наиболее часто используют марковские и полумарковские.

Марковским процессом с непрерывным временем описывают функционирование экспоненциальных СеМО. Сеть называется экспоненциальной, если входящие потоки требований в каждую СМО пуассоновские, а времена каждого этапа обслуживания, реализуемого на любой СМО сети, имеют экспоненциальное распределение. Это позволяет считать, что этапы обслуживания независимы между собой и не зависят ни от параметров входящего потока, ни от состояния сети, ни от маршрутов следования требований.

Теория экспоненциальных СеМО наиболее разработана, и ее широко применяют как для исследования сетей ПД так и для исследования мультипроцессорных вычислительных систем.

Разработаны практические формы расчета вероятностно-временных характеристик (ВВХ) таких сетей и систем.

Попытки глубокого анализа немарковских моделей сетевых систем наталкиваются на значительные трудности, которые обусловлены в частности отсутствием независимости длительностей пребывания требований в различных узлах моделей сетевых систем с нестандартными дисциплинами. Так например, при достаточно реалистическом предположении о том, что длина требования остается постоянной в процессе его передачи через узлы сети, необходимо прослеживать путь каждого требования, что делает невозможным аналитический расчет характеристики для сети с числом узлов M>2.

Анализ работ, посвященных исследованию или расчету немарковских моделей, показывает, что решения, как правило, получены алгоритмически путем сложных численных расчетов с использованием преобразований Лапласа-Стилтьеса, реализуются программно, отличаются большой трудоемкостью, либо значительными погрешностями в оценке показателей производительности информационных систем (ИС) в области средней и большой нагрузки. Поэтому для моделирования СеМО, выходящих из класса мультипликативных, используют приближенные методы.

Сравнительный анализ приближенных методов моделирования СеМО показывает, что пользоваться приближенными методами расчета СеМО необходимо с большой осторожностью, что при расчете конкретных СеМО в процессе решения различных прикладных задач представляется необходимым проведение исследований в целях оценки точности и чувствительности применяемого метода, а также проведение эксперимента по имитационному моделированию исходной СеМО для достаточно большого множества значений варьируемых параметров.

Таким образом, аналитические методы расчета характери-

стик КС базируются, как правило, на анализе экспоненциальных СеМО. При использовании этого математического аппарата удается получить аналитические модели для решения широкого круга задач исследования систем.

В настоящее время существует значительное количество учебных пособий и монографий посвященных анализу и синтезу КС с использованием аппарата СеМО, но авторы, в основном, исследуют идеальные сетевые модели. Авторам неизвестны работы, в которых бы оценивались вышеназванные сетевые характеристики в зависимости от типа и интенсивности вредоносного информационного воздействия.

Многочисленные эксперименты авторов по моделированию сетевых атак в значительной степени ухудшали производительность КС, делая ее иной раз вообще неработоспособной.

В силу этого целью данного пособия, предназначенного в первую очередь студентам и аспирантам информационных специальностей (программистам, сетевым аналитикам, специалистов по защите информации), дать систематизированный теоретический и практический материал по оценке характеристик КС в условиях воздействия вредоносных программ.

В первой главе представлена классификация вредоносных программ, которая позволяет связать конкретные разновидности ВП с характеристиками сети, на которые этот вид оказывает наибольшее влияние. Приводится сравнение воздействий различных видов и версий антивирусных программ на характеристики КС и их системные требования.

Во второй главе рассмотрены аналитические модели оценки влияния вредоносных и антивирусных программ на системные характеристики корпоративных сетей. В третьей главе излагаются принципы имитационного моделирования, предлагается имитационная модель компьютерной сети в среде GPSS World.

Глава 1. Объект изучения – компьютерная сеть

Объектом изучения в данной работе является компьютерная сеть. *Компьютерная сеть* (КС, сеть ЭВМ, вычислительная сеть (ВС)) – совокупность средств вычислительной техники и средств телекоммуникаций, реализующих соответственно две основные функции: обработку данных и передачу данных.

Любая компьютерная сеть обладает двумя важными свойствами, называемыми работоспособностью и эффективностью. *Работоспособность* КС состоит в правильном выполнении заданных функций, т.е. в правильной реализации заданного множества алгоритмов обработки информации. *Эффективность* КС заключается в ограниченности или минимальности разного рода затрат, связанных с применением КС.

Анализ эффективности компьютерной сети осуществляется путём оценки *показателей* эффективности, т.е. величин, характеризующих затраты на эксплуатацию КС. К таким величинам, например, относятся габариты КС и её устройств, быстродействие устройств, вероятность получения ошибочного результата и т.д.

Показатели, характеризующие затраты времени на получение системой каких-либо полезных результатов, называются показателями *производительности*. К их числу относятся, например, средние значения времён ответа сети на разные типы запросов, средние числа задач разного типа, решаемых системой в единицу времени, коэффициенты загрузки устройств КС и другие показатели.

Многие (если не все) показатели эффективности КС могут быть сведены к форме показателей производительности. Имея ввиду это обстоятельство, термин "производительность" иногда употребляют как равносильный термину "эффективность".

Эффективность компьютерной сети может быть охарактеризована совокупностью величин, которые можно разделить на два класса:

– параметры;

– характеристики.

1. 1 Параметры и характеристики компьютерных сетей

В качестве параметров КС выделяют:

1) структурные параметры, описывающие состав и структуру сети: количество узлов, входящих в состав сети, и их взаимосвязь; типы узлов и состав оборудования (ЭВМ и устройств); технические данные устройств (быстродействие ЦП, ёмкости ОП и ВЗУ, пропускные способности каналов связи и т.п.);

2) функциональные параметры, описывающие стратегию управления передачей данных в вычислительной сети (способ коммутации, метод доступа к каналу связи, алгоритм выбора маршрута передачи данных в сети) и стратегию управления обработкой данных в узлах (режим функционирования ВС, последовательность выполнения прикладных задач, приоритеты задач и т.п.);

3) нагрузочные параметры, описывающие взаимодействие сети с внешней средой, т.е. нагрузку, создаваемую в сети решаемыми прикладными задачами и передаваемыми в вычислительной сети данными: число типов задач, ресурсоёмкость каждой задачи, объём занимаемой памяти, длина передаваемых по сети сообщений и т.п.

Характеристики КС – это совокупность показателей эффективности (качества) сети.

Характеристики КС делятся на две группы:

– качественные;

– количественные.

К качественным характеристикам относятся:

1) операционные возможности сети, представляющие собой перечень услуг (сервис) по передаче и обработке данных, предоставляемых пользователям сети, таких как:

а) передача данных между удалёнными пользователями сети;

б) доступ к удалённым файлам;

в) доступ к разнообразным вычислительным средствам, в том числе, большим и суперЭВМ, работающим с различными операционными системами;

г) электронная почта;

д) организация распределённых баз данных;

е) возможность передачи по сети разнообразных данных;

2) масштабируемость – способность сети при её наращивании (при увеличении ресурсов) линейно увеличивать свою производительность;

3) совместимость – возможность взаимодействия в пределах одной и той же сети оборудования разных производителей.

Количественные характеристики КС делятся на:

– глобальные (характеристики производительности, оперативности, надёжности, стоимостные и др.);

– локальные.

Локальные характеристики

Локальные характеристики описывают эффективность функционирования:

– узлов и каналов связи;

– узлов обработки данных: ЭВМ и ее отдельных устройств;

– отдельных сегментов сети или частей ЭВМ, например подсистемы ввода-вывода и т.п.;

– сети в целом.

Эти характеристики могут быть разбиты на две группы: временные, отражающие временные аспекты функционирования системы, и безразмерные.

К временным характеристикам относятся:

– время ожидания передачи данных в узлах сети (перед каналом связи);

– время доставки (задержки) сообщения при передаче между двумя соседними узлами сети;

– время ожидания освобождения ресурсов ЭВМ (сервера);

– время пребывания данных в различных узлах, устройствах или подсистемах.

К безразмерным характеристикам относятся:

– коэффициенты загрузок узлов, каналов связи и устройств ЭВМ;

– число сообщений (запросов), находящихся в состоянии ожидания;

– общее число сообщений (запросов), находящихся в узлах связи, в ЭВМ или сети.

1.2 Воздействие вредоносного программного обеспечения на сетевые характеристики

К вредоносному программному обеспечению (ВПО, вредоносным программам) относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

ВПО, как и любые другие программы, требуют определенного объема ресурсов ЭВМ, на котором они исполняются, а также могут генерировать дополнительный трафик в сети. В за-

висимости от вида ВПО, создаваемая им нагрузка на ЭВМ и сеть может сильно отличаться. Так, например, классические вирусы в общем случае не создают нагрузку на сеть вовсе. Некоторые же сетевые вирусы могут совершать такое количество сетевых запросов, что вычислительная сеть может и вовсе перестать функционировать.

Таким образом, необходима некоторая классификация вирусов, которая позволила бы связать конкретные разновидности вредоносных программ с характеристиками сети, на которые этот вид оказывает наибольшее влияние.

В силу огромного разнообразия не существует единой классификации ВПО. Поэтому наиболее удобным для данной работы будет классифицировать вредоносные программы по их назначению и способам распространения одновременно, так как это позволит связать их с воздействием на те или иные характеристики вычислительной сети. По такому принципу классификации можно выделить 4 типа вредоносных программ: сетевые черви, классические вирусы, троянские программы, прочие.

Сетевые черви

К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

– проникновения на удаленные компьютеры;

– запуска своей копии на удаленном компьютере;

– дальнейшего распространения на другие компьютеры в сети.

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т. д.

Большинство известных червей распространяется в виде файлов: вложение в электронное письмо, ссылка на зараженный файл на каком-либо веб- или FTP-ресурсе в ICQ- и IRC-сообщениях и т. д.

Некоторые черви (так называемые «бесфайловые» или «пакетные» черви) распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код.

Для проникновения на удаленные компьютеры и запуска своей копии черви используют различные методы: социальный инжиниринг (например, текст электронного письма, призывающий открыть вложенный файл), недочеты в конфигурации сети (например, копирование на диск, открытый на полный доступ), ошибки в службах безопасности операционных систем и приложений.

Некоторые черви обладают также свойствами других разновидностей вредоносного программного обеспечения. Например, некоторые черви содержат троянские функции или способны заражать выполняемые файлы на локальном диске, т. е. имеют свойство троянской программы и/или компьютерного вируса.

Выделяют следующие виды сетевых червей:

1) IM-Worm, IRC-Worm – черви, распространяющиеся через различные сервисы, предназначенные для быстрого обмена сообщениями. Как правило, создают незначительную нагрузку на вычислительные ресурсы зараженной ЭВМ и сеть, поскольку осуществляют разовую отсылку сообщений, не требующую значительных ресурсов.

2) Email-Worm – почтовые черви, которые отсылают либо свои копию в виде вложения в электронных письмах, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе. Требуют значительных ресурсов зараженной ЭВМ, так

как могут анализировать файлы, находящиеся на дисках, в поисках e-mail адресов для рассылки. Также могут создавать высокую нагрузку на сеть, если тело вируса имеет большой размер и пересылается непосредственно в письме.

3) Net-Worm – обычные сетевые черви, которые распространяются через уязвимости в операционных системах и приложениях. Чаще всего незначительно нагружают сеть, однако могут выводить из строя различные программные сервисы защиты целевой ЭВМ.

4) P2P-Worm — черви, распространяющиеся через файлообменные сети и ресурсы публичного пользования. Вирус копирует себя во все доступные открытые ресурсы, в результате чего значительно нагружается вычислительная сеть машины, на которой этот ресурс расположен.

Классические вирусы

К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью:

– последующего запуска своего кода при каких-либо действиях пользователя;

– дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей, вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

– при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;

– вирус скопировал себя на съёмный носитель или заразил файлы на нем;

– пользователь отослал электронное письмо с зараженным вложением.

Некоторые вирусы содержат в себе свойства других разновидностей вредоносного программного обеспечения, например бэкдор-процедуру или троянскую компоненту уничтожения информации на диске.

Как правило, классические вирусы слабо загружают ресурсы зараженного узла и совсем не используют компьютеную сеть.

Троянские программы

В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор и передачу информации злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для массированных DoS-атак на удалённые ресурсы сети).

По вредоносному действию на компьютерную сеть и ее компоненты можно выделить следующие группы троянских программ:

1) Backdoor – троянские утилиты удаленного администрирования. Такие программы, фактически, добавляют новую операционную возможность для данной ЭВМ, а значит становится возможным произвольное использование ресурсов как самого узла, так и сети, причём заранее не возможно указать интенсивность такой нагрузки.

2) Trojan-Clicker, Trojan-Proxy – типы ВПО, которые активно используют как сеть, так и ресурсы зараженной ЭВМ. Первая группа занимается массовой генерацией различных сетевых запросов, а вторая – пересылкой полученных данных.

3) Trojan-Spy – различные шпионские программы, которые записывают данные, вводимые с клавиатуры, снимки экрана и другие подобные данные, после чего отсылают их «владельцу» вируса. Такие ВПО может незначительно использовать ВС, однако создаёт высокую нагрузку на ресурсы ЭВМ.

Другие вредоносные программы

К данной категории относят:

1) Организаторы DDoS атак, флудеры. Создают чрезвычайно большую нагрузку на вычислительную сеть и высокую на ресурсы зараженной ЭВМ.

2) Spyware-программы, Adware-программы – соответственно отсылают данные о предпочтениях пользователя и показывают рекламу в ПО. Незначительно используют ресурсы сети, но повышают нагрузку на процессор ЭВМ.

В таблице 1 представлена общая статистика воздействия ВПО на характеристики компьютерной сети (Биячуев Т.А.).

Таблица 1 - Воздействие ВПО на характеристики КС

Воздействие	Процент влияния на характеристики КС (%)
Потеря производительности	75
Компьютеры были недоступны	69
Повреждения файлов	62
Потеря доступа к файлам	49
Потеря данных	47
Потеря доверия пользователей	33
Закрытие доступа	18
Ненадежность прикладного ПО	13
Трудности с чтением файлов	12
Трудности с сохранением файлов	9
Падение системы	9
Трудности с выводом на печать	7

1.3 Воздействие антивирусного программного

обеспечения на сетевые характеристики

Методы защиты делятся на два типа - организационные и технические. *Организационные методы* направлены в первую очередь на пользователя компьютера. Их цель состоит в том, чтобы изменить поведение пользователя, ведь не секрет, что часто вредоносные программы попадают на компьютер из-за необдуманных действий пользователя. Простейший пример организационного метода - разработка правил работы за компьютером, которые должны соблюдать все пользователи.

Технические методы, наоборот, направлены на изменения в компьютерной системе. Большинство технических методов состоит в использовании дополнительных средств защиты, которые расширяют и дополняют возможности антивирусного программного обеспечения (АПО, антивирусных программ, антивирусов). Такими средствами защиты могут быть: брандмауэры - программы, защищающие от атак по сети; средства борьбы со спамом; исправления, устраняющие "дыры" в операционной системе, через которые могут проникать вирусы.

Работу АПО в системе нельзя оценивать однозначно. Во многом они сами похоже на вирусы. Так, антивирусы используют, несомненно, больше ресурсов компьютера, чем требуются для своей работы вирусы, от которых он потенциально защищает ЭВМ. Зачастую антивирусы тем или иным образом ограничивают функциональные возможности ПО, установленного на ЭВМ, например, затрудняют открытие вложений электронной почты. Для эффективной работы антивирусных программ требуется постоянное их обновление, что может создавать значительную нагрузку на вычислительную сеть.

Для вычисления производительности компьютера, затрачиваемой АПО для своей работы, используем следующую методику. Примем за производительность, необходимую антивиру-

су, равной производительности ЭВМ, заявленной в качестве минимальных требований для запуска программы. Требования наиболее популярных современных АПО представлены в таблице 2.

Таким образом, усредненные данные о требованиях антивирусов для работы в наиболее популярных операционных системах следующие: 400 МГц процессорной частоты, 256 Мб памяти, до 180 Мб места на жестком диске.

Таблица 2 - Системные требования АПО

Антивирусная программа	Процессор	Память	Жесткий диск
Norton AntiVirus 2008	300 МГц	256 Мб	300 Мб
avast! Professional	Pentium 4	256 Мб	50 Мб
ESET NOD32	32-разрядный (x86) и 64-разрядный (x64) Intel, AMD	33-38 Мб	16-78 Мб
Антивирус Касперского 7.0	Intel Pentium 300 МГц	128 Мб	50 Мб

По приблизительным оценкам специалистов, среднестатистическая современная офисная система имеет процессор с частотой 2 ГГц, 256 Мб памяти и дисковым накопителем несколько десятков гигабайт, то есть совпадает по основным показателям с узлами заданной локальной сети. Поскольку объем свободного пространства на жестком диске значительно превышает требования антивирусов, его можно не учитывать. Таким образом, получается, что среднестатистический современный антивирус будет использовать порядка 20% ресурсов компьютера.

Влияние на производительность КС разных антивирусных

программ (и даже разных версий одного и того же ПО) не может быть одинаковым. Одни из них лучше оптимизированы, другие снижают нагрузку, уменьшая тщательность проверки.

Сравнение воздействий АПО на характеристики компьютера приведено в таблице 3. В качестве испытательного стенда для изучения влияния антивирусов использовался компьютер со следующими характеристиками: процессор: Intel Core 2 Duo T7600, 2,33 ГГц; память: 2048 Мб, DDR2-533; видео: NVIDIA GeForce Go 7600, 256 Мб; жёсткий диск: 320 (160 +160 RAID) Гб; дисплей: 17"TFT WUXGA (1920x1200); звуковая карта: TruSurround XT, Harman Kardon; оптические устройства: HD DVD-RW; порты: PCMCIA Type II; 4xUSB 2.0; VGA; S-Video; IEEE 1394. Устройства связи: FM 56K, LAN 10/100, Wi-Fi, Bluetooth, ТВ-тюнер.

Программное обеспечение, учитываемое при тестировании: Windows XP Media Center Edition, 3DMark05, COSBI OpenSourceMark 1.0 beta 7a, Microsoft Bootvi (измерение времени загрузки операционной системы).

Перед инсталляцией каждого антивирусного продукта средствами утилиты System Restore производился откат конфигурации операционной системы в изначальное состояние, а сами тесты прогонялись десятки раз.

Конкретные результаты зависят от конфигурации компьютера, но общая картина, как правило, сохраняется.

Проводимые тесты:

- измерение времени (в секундах) загрузки операционной системы средствами утилиты Bootvis;

- измерение времени (в секундах) копирования одиночных файлов разного размера (100 Мб и 1000 Мб) средствами бенчмарк-пакета COSBI OpenSourceMark 1.0;

- оценочный анализ (в баллах) быстродействия системы при выполнении таких операций, как архивирование данных,

кодирование мультимедийных файлов в формат MP3 и загрузка веб-страниц, хранящихся на жёстком диске компьютера (для проведения тестов использовался инструмент COSBI OpenSourceMark 1.0).

Таблица 3 - Влияние АПО на характеристики ЭВМ

	Время загрузки системы, с	Копирование файла 100 Мб, с	Копирование файла 1000 Мб, с	Сжатие ZIP,баллы	Загрузка веб-страниц*, баллы
Без антивируса	45,62	2,69	25,75	984	1745
Антивирус Касперского 7.0 (настройки по умолчанию)	62,23	2,8	28,14	956	1541
Антивирус Касперского 7.0 (максимальная защита)	63,35	2,4	31,07	964	1525
Trend Micro Internet Security Pro (настройки по умолчанию)	58,96	3,15	46	942	1414
Trend Micro Internet Security Pro (максимальная защита)	57,13	5,05	59,28	775	1424
Dr.Web 4.44 (настройки по умолчанию)	51,63	2,84	41,95	978	1663
Dr.Web 4.44 (мак-	58,	2,9	42,	620	165

симальная защита)	28	3	91		5
Panda Antivirus 2008 (настройки по умолчанию)	55,56	3,03	43,69	946	1705
Panda Antivirus 2008 (максимальная защита)	54,84	3,05	43,55	839	1707
Eset NOD32 Antivirus (настройки по умолчанию)	50,82	3,23	41,53	948	1701
Eset NOD32 Antivirus (максимальная защита)	52,11	3,24	41,58	943	1705
avast! 4 Home Edition (настройки по умолчанию)	66,95	3	43,62	937	1665
avast! 4 Home Edition (максимальная защита)	70,44	3,23	42,7	926	1668
Norton Antivirus 2008 (настройки по умолчанию)	62,37	3,16	43,56	937	1559
Norton Antivirus 2008 (максимальная защита)	73,02	3,4	43	978	1575
Антивирус Stop! 4.10 Pro Edition (настройки по умолчанию)	46,67	3,4	42,88	941	1699
AVG Anti-Virus 7.5 (настройки по умолчанию)	55,82	3,3	43,14	942	1711
AVG Anti-Virus 7.5 (максимальная защита)	55,7	3,5	43,21	937	1702
CA Anti-Virus 8.1	95,	3,2	41,	939	170

(настройки по умолчанию)	35	91	1

* С жесткого диска компьютера

Результаты тестирования получились достаточно показательными. К примеру, отчётливо видно, как велико влияние антивирусных продуктов на время загрузки Windows: практически все они оттянули старт операционной системы на десять и более секунд. В основном АПО оказывают нагрузку на процессор и оперативную память.

Контрольные вопросы и задания

1. Рассмотрите классификации вредоносных программ по различным признакам.
2. Проведите исследование влияния современных вредоносных программ на сетевые характеристики, в том числе и производительность компьютерных систем, с помощью натурных экспериментальных установок и результатов уже опубликованных тестов. Количественно оцените изменение характеристик.
3. Рассмотрите перспективы создания антивирусных программ, способных максимально защитить компьютерные системы от вредоносных программ без ухудшения характеристик.
4. Проведите исследование воздействия различных средств защиты от вредоносных программ (по мимо антивирусного программного обеспечения) на сетевые характеристики.
5. Каким образом следует выбирать средства противодействия вредоносным программам на объекте защиты.

Глава 2. Аналитические модели компьютерной сети

Решая задачу оценки характеристик компьютерных сетей в условиях воздействия вредоносных программ, необходимо учитывать случайную природу многих факторов, от которых зависят характеристики КС. Случайными часто являются моменты поступления в сеть требований, объёмы подлежащей обработке информации, последовательность необходимых для ее обработки операций. Сложность структуры КС и необходимость учёта случайных факторов делают задачу оценки характеристик сложной, причём по мере прогресса вычислительной техники и вредоносных информационных воздействий на КС сложность этой задачи возрастает. Поэтому широкое распространение для оценки характеристик сети получил метод математического моделирования.

Моделирование - один из наиболее распространенных методов исследования процессов функционирования сложных систем. Наиболее распространенными из методов построения математических моделей являются *системы массового обслуживания* (СМО).

Усложнение структур и режимов реальных КС затрудняет применение классических методов *теории массового обслуживания* (ТМО) ввиду возрастающей размерности решаемых задач. Одним из возможных путей преодоления размерности является использование моделей в форме *сетей массового обслуживания* (СеМО).

СеМО представляет собой совокупность конечного числа обслуживающих узлов, в которой циркулируют заявки, переходящие в соответствии с маршрутной матрицей из одного узла в другой. Узел всегда является разомкнутой системой массового обслуживания (СМО). При этом отдельные СМО отображают

функционально самостоятельные части реальной компьютерной сети предприятия, связи между СМО - структуру сети, а требования, циркулирующие по СеМО, - составляющие материальных потоков (сообщения (пакеты) в сети).

В теории СеМО фундаментальным является понятие состояния сети. Важнейшая характеристика сетей МО - вероятности их состояний. Для определения вероятностей состояний СеМО исследуют протекающий в сети случайный процесс. В качестве моделей протекающих в СеМО процессов наиболее часто используют марковские.

Марковским процессом с непрерывным временем описывают функционирование экспоненциальных СеМО. Сеть называется *экспоненциальной*, если входящие потоки требований в каждую СМО пуассоновские, а времена каждого этапа обслуживания, реализуемого на любой СМО сети, имеют экспоненциальное распределение. Это позволяет считать, что этапы обслуживания независимы между собой и не зависят ни от параметров входящего потока, ни от состояния сети, ни от маршрутов следования требований.

Аналитические модели расчета характеристик КС базируются, как правило, на анализе экспоненциальных СеМО. При использовании этого математического аппарата удается получить аналитические модели для решения широкого круга задач исследования компьютерных сетей.

2.1 Модель замкнутой сети

Пусть дана замкнутая сеть, состоящая из K систем массового обслуживания (рис. 1). В *замкнутой* СеМО циркулирует фиксированное число заявок, а внешний независимый источник отсутствует.

Пусть N – количество пакетов, циркулирующих в сети;

$P_R=(p_{ji})$ – маршрутная матрица; m_i – количество обрабатывающих конвейеров в i-м узле; τ_i – среднее время обработки пакета в одном конвейере i-го узла $\forall i = \overline{1, K}$.

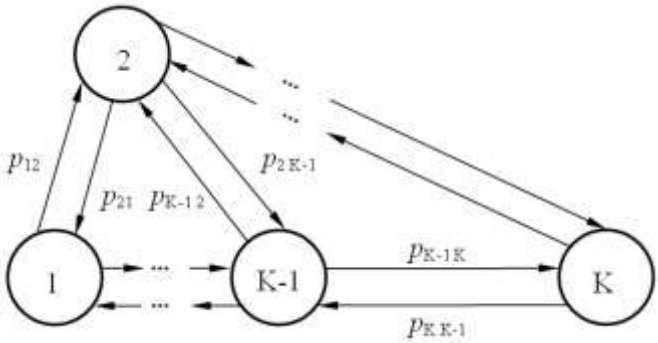

Рисунок 1 - Граф замкнутой сети

Требуется: найти все возможные состояния сети в целом и состояния каждого узла в отдельности; рассчитать вероятности этих состояний $P_i(n_i)$; найти среднее число пакетов в узле L_i; интенсивности потоков поступающих пакетов λ_i; среднее время пребывания пакета в узле T_i и среднее время цикла V_i.

В общем случае сеть задается стохастической маршрутной матрицей:

$$P_R = \begin{pmatrix} p_{11} & p_{12} \dots p_{1K} \\ p_{21} & p_{22} \dots p_{2K} \\ \dots\dots\dots\dots\dots \\ p_{K1} & p_{K2} \dots p_{KK} \end{pmatrix}, \qquad (1)$$

где p_{ij} – вероятность пересылки пакета из i-го узла в j-й узел, причём $\sum_{j=1}^{K} p_{ij} = 1 \ \forall i = \overline{1, K}$.

Обозначим как $\lambda_i = e_i \Lambda$ интенсивность потока пакетов, поступающих в i-й узел, где e_i – передаточные коэффициенты. λ_i – это физическая величина, которую можно измерить.

Физический смысл интенсивности потока событий – это среднее число событий, приходящееся на единицу времени (число заявок в единицу времени), размерность – 1/время.

Для стационарного режима интенсивность потока, входящего в узел, равна интенсивности исходящего. Составим систему уравнений:

$$\lambda_j = \sum_{i=1}^{K} \lambda_i p_{ij} \quad \forall i = \overline{1, K}$$

Учитывая, что $\lambda_i = e_i \Lambda$ и $\lambda_j = e_j \Lambda$, сократим на Λ: $e_j = \sum_{i=1}^{K} e_i p_{ij}$, или в развернутом виде:

$$\begin{cases} (p_{11} - 1)e_1 + p_{21}e_2 + \ldots + p_{K1}e_K = 0 \\ p_{12}e_1 + (p_{22} - 1)e_2 + \ldots + p_{K2}e_K = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ p_{1K}e_1 + p_{2K}e_2 + \ldots + (p_{KK} - 1)e_K = 0 \end{cases} \qquad (2)$$

Система линейных уравнений (2) в матричной форме: $P_1 E = 0$, где матрица P_1 получена путем транспонирования матрицы (1) и уменьшением элементов главной диагонали на 1:

$$P_1 = \begin{pmatrix} p_{11} - 1 & p_{21} & \ldots & p_{K1} \\ p_{12} & p_{22} - 1 & \ldots & p_{K2} \\ \ldots & \ldots & \ldots & \ldots \\ p_{1K} & p_{2K} & \ldots & p_{KK} - 1 \end{pmatrix} \text{ и } E = \begin{pmatrix} e_1 \\ e_2 \\ \ldots \\ e_K \end{pmatrix}.$$

Чтобы получить единственное решение, положим $e_1 = 1$. Тогда сложим 1-ую строку матрицы P_1 почленно с k-й, где $k = \overline{2, K}$ и получим:

$$P_2 E = Q, \tag{3}$$

где $P_2 = \begin{pmatrix} p_{21} + p_{22} - 1 & \ldots & p_{K1} + p_{K2} \\ p_{21} + p_{23} & \ldots & p_{K1} + p_{K3} \\ \ldots & \ldots & \ldots \\ p_{21} + p_{2K} & \ldots & p_{K1} + p_{KK} - 1 \end{pmatrix}$ размерностью

$K - 1$ и $Q = \begin{pmatrix} p_{11} - 1 + p_{12} \\ p_{11} - 1 + p_{13} \\ \ldots \\ p_{11} - 1 + p_{1K} \end{pmatrix}$.

Применив Метод Гаусса к (3), найдем передаточные коэффициенты $e_2, e_3, \ldots, e_K$.

Рассмотрим узлы замкнутой сети по отдельности (рис. 2).

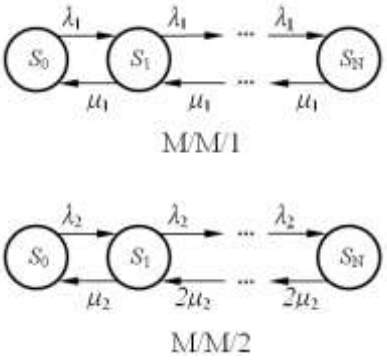

Рисунок 2 - Схемы узлов замкнутой сети

Обозначим как $\mu_i = 1/\tau_i$ интенсивность обработки пакетов в i-м узле, где τ_i – среднее время обработки пакета в i-м узле, распределённое по экспоненциальному закону: $P(t) = \mu e^{-\mu t}$, $t \geq 0$.

Возможные состояния 1-го узла (1 конвейер) $\{S_k\} = \{S_0, S_1, S_2, \ldots, S_N\}$, где k – число пакетов (обрабатывающихся или ожидающих) в узле. Процесс блуждания по этим состояниям будет Марковским процессом гибели и размножения. Вероятность нахождения 1-го узла при стационарном режиме в состоянии S_k обозначим как $P_1(k)$. Выразим вероятности этих состояний через $P_1(0)$: $P_1(1) = \frac{\lambda_1}{\mu_1} P_1(0)$, $P_1(2) = \frac{\lambda_1^2}{\mu_1^2} P_1(0)$, $P_1(3) = \frac{\lambda_1^3}{\mu_1^3} P_1(0)$ и т.д, причём $\sum_{n=0}^{N} P_1(n) = 1$. Выражение для числителя получаются перемножением интенсивностей поступления пакетов (размножение), для знаменателя – интенсивностей их обслуживания (гибель). $P_1(0)$ пока остаётся неизвестным.

Рассмотрим 2-й узел с 2-мя конвейерами. Если в узле 2 конвейера, то узел начинает обрабатывать пакеты с удвоенной интенсивностью (задействованы оба конвейера), когда в нем находится 2 пакета и более.

$$P_2(1) = \frac{\lambda_2}{\mu_2} P_2(0), \quad P_2(2) = \frac{\lambda_2^2}{2\mu_2^2} P_2(0), \quad P_2(3) = \frac{\lambda_2^3}{4\mu_2^3} P_2(0)$$

и т.д, причём $\sum_{n=0}^{N} P_2(n) = 1.$

В общем случае, вероятность нахождения *i*-го узла в состоянии S_k:

$$P_i(n) = \frac{\lambda_i^n}{\mu_i^n \beta_i(n)} P_i(0) \qquad \forall i = \overline{1, K}, \tag{4}$$

где $\beta_i(n) = \begin{cases} n!, n \le m \\ m! m^{n-m}, n > m \end{cases}$, m – число конвейеров в *i*-м узле.

Рассмотрим все возможные состояния сети $\vec{n} = (n_1, n_2, \ldots, n_K) : n_1 + n_2 + \ldots + n_K = N$, где n_i – число пакетов в узле. Обозначим множество всех состояний сети как $S(N,K)$. По теореме декомпозиции (Джексона), в стационарном режиме состояние всей сети определяется состоянием её узлов:

$$P(\vec{n}) = \frac{\prod_{i=1}^{K} P_i(n_i)}{\sum_{\vec{n}' \in S(N,K)} \prod_{i=1}^{K} P_i(n_i')} \quad \forall \vec{n} = (n_1, n_2, \ldots, n_K) \in S(N,K),$$

где $P_i(n_i)$ – вероятность нахождения *i*-го узла в состоянии S_{n_i}, а суммирование проводится по всему множеству состояний сети $S(N,K)$. Подставим сюда выражения для $P_i(n_i)$, сократим дробь на $P_1(0), P_2(0), \ldots, P_K(0)$.

Подставляя сюда выражения для λ_i и учитывая, что $n_1 + n_2 + \ldots + n_K = N$, сократим дробь на Λ^N. В результате получаем:

$$P(\vec{n}) = \frac{\prod_{i=1}^{K} \frac{e_i^{n_i}}{\mu_i^{n_i} \beta_i(n_i)}}{\sum_{\vec{n}' \in S(N,K)} \prod_{i=1}^{K} \frac{e_i^{n_i'}}{\mu_i^{n_i'} \beta_i(n_i')}} \quad \forall \vec{n} = (n_1, n_2, \ldots, n_K) \in S(N,K) \tag{5}$$

Когда все величины известны, можно рассчитать вероятности всех состояний сети $S(N,K)$. Можно убедиться, что

$$\sum_{\vec{n}\in S(N,K)} P(\vec{n}) = 1.$$

Найдём также $P_i(k)$ – все вероятности нахождения каждого i-го узла в состоянии S_k:

$$P_i(k) = \sum_{\substack{\vec{n}'\in S(N,K):\\ n'_i=k}} P(\vec{n}') \quad \forall i = \overline{1,K}\,,\ \forall k = \overline{0,N}\,.$$

Здесь суммирование проводится только по тем состояниям из множества $S(N,K)$, для которых в i-м узле находится ровно k пакетов. Убедимся, что $\sum_{n=0}^{N} P_i(n) = 0 \quad \forall i = \overline{1,K}$.

Среднее число пакетов в i-м узле находится как математическое ожидание количества пакетов в i-м узле: $L_i = \sum_{n=0}^{N} nP_i(n)$ $\forall i = \overline{1,K}$. Можно убедиться, что $\sum_{i=1}^{K} L_i = N$.

Интенсивность λ_i входящего в i-м узел потока в стационарном режиме будет равна интенсивности выходящего потока (т.е. производительности узла). Эта величина находятся как математическое ожидание интенсивности потока обработанных пакетов: $\lambda_i = \sum_{n=0}^{N} \mu_i(n)P_i(n) \quad \forall i = \overline{1,K}$, где $\mu_i(n)$ – общая интенсивность обработки n пакетов в i-м узле:

$$\mu_i(n) = \begin{cases} n\mu_i, n \le m \\ m\mu_i, n > m \end{cases}, \quad m \text{ – число конвейеров в } i\text{-м узле.}$$

Можно убедиться, что $\frac{\lambda_1}{e_1} = \frac{\lambda_2}{e_2} = \ldots = \frac{\lambda_K}{e_K}$. Теперь сред-

нее время пребывания пакета в i-м узле можно рассчитать по теореме Литтла: $T_i = \frac{L_i}{\lambda_i} \quad \forall i = \overline{1, K}$. Найдём также среднее время цикла V_i – среднее время между моментом выхода пакета из i-го узла до момента первого поступления этого пакета в тот же узел:

$$V_i = \sum_{\substack{j=1 \\ j \neq i}}^{K} \frac{e_j}{e_i} T_j \qquad \forall i = \overline{1, K},$$

где $\frac{e_j}{e_i}$ – среднее число посещений j-го узла между двумя последовательными посещениями i-го узла. Учитывая, что $\frac{\lambda_i}{e_i} = \frac{\lambda_j}{e_j}$, $L_j = T_j \lambda_j$ и $\sum_{\substack{j=1 \\ j \neq i}}^{K} L_j = N - L_i$, получаем $V_i = \frac{N - L_i}{\lambda_i}$, $\forall i = \overline{1, K}$.

Алгоритм расчета характеристик замкнутой сети

Шаг 1. Задать начальные значения характеристик сети:

1) N - количество пакетов, циркулирующих в сети;

2) маршрутную матрицу P_R;

3) количество обрабатывающих конвейеров в каждом узле: $m_1, m_2, m_3, m_4, m_5, m_6, m_7$;

4) среднее время обработки пакета в одном конвейере каждого узла: $\tau_1, \tau_2, \tau_3, \tau_4, \tau_5, \tau_6, \tau_7$.

Шаг 2. Получить систему линейных уравнений в матричной форме (3).

Шаг 3. Применить метод Гаусса к (3), чтобы найти передаточные коэффициенты $e_2, e_3, \ldots, e_K$.

Шаг 4. Найти множество $S(N,K)$ всех состояний сети.

Шаг 5. Получить возможные состояния $\{S_k\} = \{S_0, S_1, S_2, \ldots, S_N\}$ для каждого узла, где k – число пакетов (обрабатывающихся или ожидающих) в узле и рассчитать вероятности $P_i(n)$ этих состояний.

Шаг 6. Рассчитать среднее число пакетов как математическое ожидание количества пакетов в *i*-м узле: $L_i = \sum_{n=0}^{N} nP_i(n)$ $\forall i = \overline{1, K}$.

Шаг 7. Рассчитать интенсивность входящего в каждый узел потока: $\lambda_i = \sum_{n=0}^{N} \mu_i(n) P_i(n) \quad \forall i = \overline{1, K}$, где $\mu_i(n)$ – общая интенсивность обработки n пакетов в *i*-м узле: $\mu_i(n) = \begin{cases} n\mu_i, n \le m \\ m\mu_i, n > m \end{cases}$, m – число конвейеров в *i*-м узле.

Шаг 8. По теореме Литтла рассчитать среднее время пребывания пакета в *i*-м узле: $T_i = \frac{L_i}{\lambda_i} \quad \forall i = \overline{1, K}$. Конец алгоритма.

Рассмотрим предложенный алгоритм расчета характеристик замкнутой сети на примере компьютерной сети, построен-

ной по технологии Ethernet, в которой каждый узел имеет линию связи с любым другим узлом данной сети (рис. 3).

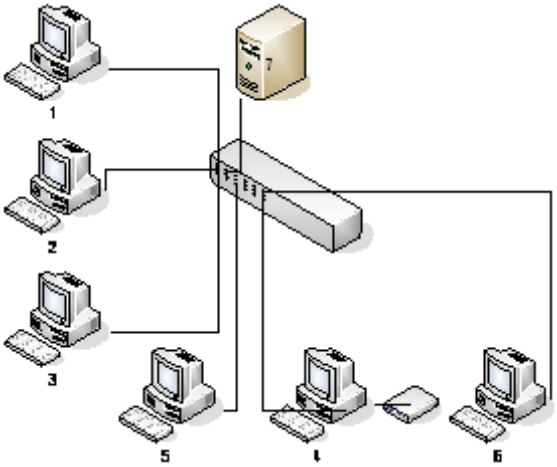

Рисунок 3 - Топология КС

Компьютерная сеть состоит из семи узлов: 6 персональных компьютеров и сервер (таблица 1).

Таблица 1 - Аппаратные характеристики узлов сети

Узел КС	Количество	Аппаратное обеспечение
Компьютер	2	512Mb ОЗУ; процессор Intel Pentium 4, 2Ghz
Компьютер	2	256Mb ОЗУ; процессор Intel Celeron, 2Ghz
Компьютер	2	128Mb ОЗУ; процессор Intel Pentium P3, 500 Mhz
Система AlphaServer 800 5/400	1	768Mb ОЗУ; процессор Alpha 21164, 400 Mhz

В рамках рассматриваемой модели КС (рис.3) имеет следующие характеристики:

1) $K = 7$ – количество СМО.

2) $N = 8$ – количество запросов (пакетов), циркулирующих в сети.

3) $P_R = \begin{pmatrix} 0,1 & 0,2 & 0,1 & 0,3 & 0 & 0,1 & 0,2 \\ 0,1 & 0,1 & 0,3 & 0,2 & 0,1 & 0,1 & 0,1 \\ 0,2 & 0,1 & 0 & 0,1 & 0,1 & 0,4 & 0,1 \\ 0,1 & 0,2 & 0,1 & 0 & 0,1 & 0,1 & 0,4 \\ 0,1 & 0,1 & 0,1 & 0,1 & 0,4 & 0,1 & 0,1 \\ 0,2 & 0,3 & 0 & 0,1 & 0 & 0,3 & 0,1 \\ 0,2 & 0,1 & 0,1 & 0,1 & 0,2 & 0,2 & 0,1 \end{pmatrix}$ - маршрутная матрица.

4) $m_1 = 1$; $m_2 = 1$; $m_3 = 1$; $m_4 = 1$; $m_5 = 1$; $m_6 = 1$; $m_7 = 1$ – количество обрабатывающих конвейеров в каждом узле.

5) $\tau_1 = 0,5$; $\tau_2 = 0,5$; $\tau_3 = 0,7$; $\tau_4 = 0,7$; $\tau_5 = 1$; $\tau_6 = 1$; $\tau_7 = 0,3$ – среднее время обработки пакета в одном конвейере каждого из семи узлов.

С целью выявления влияния вредоносных и антивирусных программ на локальные характеристики замкнутой сети были проведены следующие мероприятия:

1. Моделирование сети в условиях отсутствия вредоносных и антивирусных программ (таблица 2).

Таблица 2 - Характеристики сети в условиях отсутствия вредоносных и антивирусных программ

Среднее число пакетов в узле	Интенсивность входящего в узел потока	Среднее время пребывания пакета в узле
L_1 = 0,552	λ_1 = 0,727	T_1 = 0,759
L_2 = 0,675	λ_2 = 0,829	T_2 = 0,815
L_3 = 0,561	λ_3 = 0,525	T_3 = 1,069
L_4 = 0,821	λ_4 = 0,666	T_4 = 1,232
L_5 = 1,290	λ_5 = 0,596	T_5 = 2,167
L_6 = 3,801	λ_6 = 0,924	T_6 = 4,111
L_7 = 0,300	λ_7 = 0,777	T_7 = 0,386

2. Моделирование сети под воздействием только вредоносных программ (таблица 3) при N = 16. Количество пакетов N увеличили в 2 раза для имитации атаки на сеть.

Таблица 3 - Характеристики сети под воздействием только вредоносных программ

Среднее число пакетов в узле	Интенсивность входящего в узел потока	Среднее время пребывания пакета в узле
L_1 = 0,643	λ_1 = 0,784	T_1 = 0,820
L_2 = 0,804	λ_2 = 0,893	T_2 = 0,900
L_3 = 0,654	λ_3 = 0,566	T_3 = 1,156
L_4 = 1,004	λ_4 = 0,718	T_4 = 1,399
L_5 = 1,755	λ_5 = 0,642	T_5 = 2,734
L_6 = 10,804	λ_6 = 0,997	T_6 = 10,842
L_7 = 0,335	λ_7 = 0,837	T_7 = 0,400

3. Моделирование сети под воздействием только антивирусных программ (таблица 4). Положим, что производительность конвейеров, вследствие работы антивирусов, снижается на 20%, то есть уменьшается средняя интенсивность обработки пакета в одном конвейере каждого узла μ_i .

Учитывая, что $\mu_i = 1/\tau_i$ изменили среднее время обработки запроса в конвейере каждого из семи узлов: τ_1 = 0,625; τ_2 = 0,625; τ_3 = 0,874; τ_4 = 0,874; τ_5 = 1,250; τ_6 = 1,250; τ_7 = 0,375.

Таблица 4 - Характеристики под воздействием только антивирусных программ

Среднее число пакетов в узле	Интенсивность входящего в узел потока	Среднее время пребывания пакета в узле
L_1 = 0,552	λ_1 = 0,582	T_1 = 0,949
L_2 = 0,676	λ_2 = 0,663	T_2 = 1,019
L_3 = 0,561	λ_3 = 0,420	T_3 = 1,334
L_4 = 0,819	λ_4 = 0,533	T_4 = 1,537
L_5 = 1,291	λ_5 = 0,476	T_5 = 2,708
L_6 = 3,802	λ_6 = 0,740	T_6 = 5,140
L_7 = 0,300	λ_7 = 0,622	T_7 = 0,481

Таким образом, среднее время обработки запроса в узле:

– в условиях отсутствия вредоносных и антивирусных программ: 1,506 условных единиц времени;

– под воздействием только вредоносных программ: 2,607 условных единиц времени;

– под воздействием только антивирусных программ: 1,882 условных единиц времени.

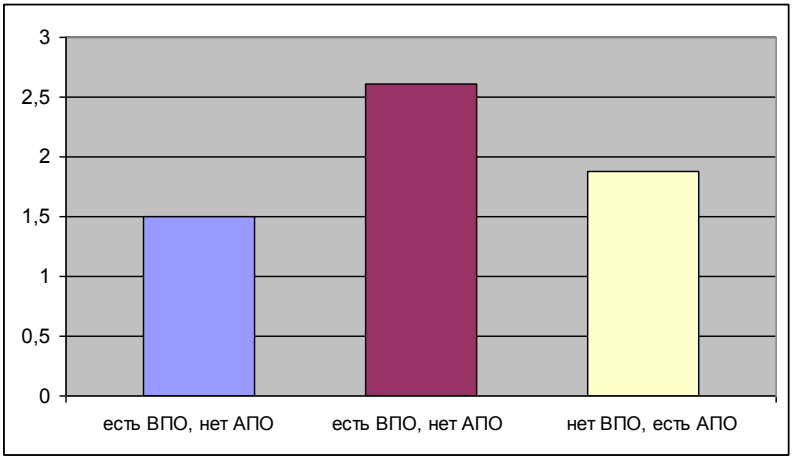

Рисунок 4 - Среднее время обработки запроса в замкнутой сети

Следовательно, под воздействием вредоносных программ среднее время обработки запроса в рассматриваемой сети увеличилось на 73,10%, а под воздействием средств защиты – на 24,97% (рис. 4).

2.2 Модель незамкнутой сети

Пусть дана незамкнутая сеть, состоящая из источника пакетов (узел 0) и K СМО M/M/m_1/∞, M/M/m_2/∞, …, M/M/m_K/∞ (рис.5). *Незамкнутая сеть* – это такая отрытая сеть, в которую заявки поступают из внешней среды и уходят после обслуживания из сети во внешнюю среду. Другими словами, особенностью незамкнутой СеМО является наличие одного или нескольких независимых внешних источников, которые генерируют заявки, поступающие в сеть, независимо от того, сколько заявок уже находится в сети. В любой момент времени в открытой СеМО может находиться произвольное число заявок.

Заданы $P_R=(p_{ji})$ – маршрутная матрица, μ_i – средняя ин-

тенсивность обработки пакета в одном конвейере i-го узла, λ_0 – интенсивность входящего в сеть потока пакетов.

Требуется: найти интенсивности потоков поступающих пакетов λ_i, минимально необходимое число конвейеров в каждом узле m_i, среднюю длину очереди r_i, среднее число пакетов в узле L_i, среднее время пребывания пакета в узле T_i, среднее число пакетов в сети N и среднее время пребывания пакета в сети T.

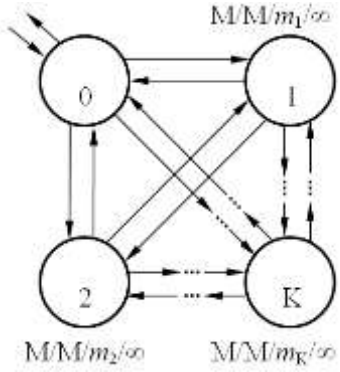

Рисунок 5 - Схема незамкнутой сети

В общем случае сеть задается стохастической маршрутной матрицей:

$$P_R = \begin{pmatrix} 0 & p_{01} & p_{02} & \dots & p_{0K} \\ p_{10} & p_{11} & p_{12} & \dots & p_{1K} \\ p_{20} & p_{21} & p_{22} & \dots & p_{2K} \\ \dots & \dots & \dots & \dots & \dots \\ p_{K0} & p_{K1} & p_{K2} & \dots & p_{KK} \end{pmatrix}, \quad (6)$$

где p_{ij} – вероятность пересылки пакета из i-го узла в j-й узел, причём $\sum_{j=0}^{K} p_{ij} = 1 \ \forall i = \overline{0, K}$.

Обозначим как $\lambda_i = e_i \lambda_0$ интенсивность потока пакетов, поступающих в i-й узел, где e_i – передаточные коэффициенты.

Физический смысл интенсивности потока событий – это среднее число событий, приходящееся на единицу времени (число заявок в единицу времени), размерность – 1/время.

Для стационарного режима интенсивность потока, входящего в узел, равна интенсивности исходящего. Составим систему уравнений:

$$\lambda_i = \sum_{j=0}^{K} \lambda_j p_{ij} \quad \forall i = \overline{0, K}.$$

Учитывая, что $\lambda_i = e_i \lambda_0$ и $\lambda_j = e_j \lambda_0$, получим: $e_i = \sum_{j=0}^{K} e_j p_{ij}$, или в развернутом виде:

$$\begin{cases} -e_0 + p_{10} e_1 + p_{20} e_2 + \ldots + p_{K0} e_K = 0 \\ p_{01} e_0 + (p_{11} - 1) e_1 + p_{21} e_2 + \ldots + p_{K1} e_K = 0 \\ p_{02} e_0 + p_{12} e_1 + (p_{22} - 1) e_2 + \ldots + p_{K2} e_K = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ p_{0K} e_0 + p_{1K} e_1 + p_{2K} e_2 + \ldots + (p_{KK} - 1) e_K = 0 \end{cases} \qquad (7)$$

Система линейных уравнений (7) в матричной форме: $P_1 E = 0$, где матрица P_1 получена путем транспонирования матрицы (6) и уменьшением элементов главной диагонали на 1:

$$P_1 = \begin{pmatrix} -1 & p_{10} & p_{20} & \ldots & p_{K0} \\ p_{01} & p_{11} - 1 & p_{21} & \ldots & p_{K1} \\ p_{02} & p_{12} & p_{22} - 1 & \ldots & p_{K2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ p_{0K} & p_{1K} & p_{2K} & \ldots & p_{KK} - 1 \end{pmatrix} \text{ и } E = \begin{pmatrix} e_0 \\ e_1 \\ e_2 \\ \ldots \\ e_K \end{pmatrix}.$$

Чтобы получить единственное решение, положим $e_0 = 1$. Тогда сложим 0-ую строку матрицы P_1 почленно с k-й, где $k = \overline{1, K}$ и получим:

$$P_2 E = Q, \tag{8}$$

где $P_2 = \begin{pmatrix} p_{10} + p_{11} - 1 & \dots & p_{K0} + p_{K1} \\ p_{10} + p_{12} & \dots & p_{K0} + p_{K2} \\ \dots & \dots & \dots \\ p_{01} + p_{1K} & \dots & p_{K0} + p_{KK} - 1 \end{pmatrix}$ и $Q = \begin{pmatrix} 1 - p_{01} \\ 1 - p_{02} \\ \dots \\ 1 - p_{0K} \end{pmatrix}$.

Применив Метод Гаусса к (8), найдем передаточные коэффициенты $e_1, e_2, \dots, e_K$. Подставим найденные значения e_i в исходную систему и убедимся, что уравнения обращаются в верные равенства.

Теперь можем найти интенсивность потока пакетов, поступающих в i-й узел:

$$\lambda_i = e_i \lambda_0 \quad \forall i = \overline{1, K}.$$

Рассмотрим один из узлов сети для общего случая (рис. 6).

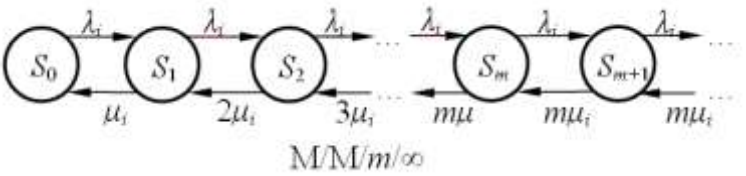

Рисунок 6 - Схема узла сети в общем случае

Допустим, что он имеет m конвейеров и неограниченную очередь. Возможными состояниями этого узла будут $\{S_k\}=\{S_0, S_1, S_2, \dots, S_m, S_{m+1}, \dots\}$, где k – число пакетов (обрабатываю-

щихся или ожидающих) в узле. Процесс блуждания по этим состояниям будет Марковским процессом гибели и размножения. Вероятность нахождения узла при стационарном режиме в состоянии S_k обозначим как $P_i(k)$. Выразим вероятности этих состояний через $P_i(0)$ (таблица 5).

Таблица 5 - Вероятности нахождения узла в различных состояниях

n	$P_i(n)$	$r_i(n)$	$k_i(n)$
0	$P_i(n)$	0	0
1	$P_i(0)\frac{\lambda_i}{\mu_i}$	0	1
…	…	…	…
m	$P_i(0)\frac{\lambda_i^{\,m}}{m!\,\mu_i^{\,m}}$	0	m
m+1	$P_i(0)\frac{\lambda_i^{\,m+1}}{m!\,m\mu_i^{\,m+1}}$	1	m
m+2	$P_i(0)\frac{\lambda_i^{\,m+2}}{m!\,m^2\mu_i^{\,m+2}}$	2	m
…	…	…	…

Выражения для числителя получаются перемножением интенсивностей поступления пакетов (размножение), для знаменателя – интенсивностей их обслуживания (гибель). В общем случае:

$$P_i(n) = \frac{\lambda_i^n}{\mu_i^n \beta_i(n)} P_i(0) \;\forall i = \overline{1, K}, \qquad (9)$$

где $\beta_i(n) = \begin{cases} n!, n \le m \\ m!\, m^{n-m}, n > m \end{cases}$, m – число конвейеров в i-м узле.

Учитывая, что $\sum_{n=0}^{\infty} p_i(n) = 1$, получим

$$P_i(0)\left(+ \frac{\lambda_i}{\mu_i} + \frac{\lambda_i^{\,2}}{2!\,\mu_i^{\,2}} + ... + \frac{\lambda_i^{\,m}}{m!\,\mu_i^{\,m}} + \frac{\lambda_i^{\,m+1}}{m!\,m\mu_i^{\,m+1}} + \right.$$

$$\left. + \frac{\lambda_i^{\,m+2}}{m!\,m^2\mu_i^{\,m+2}} + ... \right) = 1\cdot$$

Введем обозначения $\rho_i = \frac{\lambda_i}{\mu_i}$ и $\chi_i = \frac{\lambda_i}{m\mu_i}$, тогда:

$$P_i(0)\left(1 + \rho_i + \frac{\rho_i^{\,2}}{2!} + ... + \frac{\rho_i^{\,m}}{m!} + \frac{\rho_i^{\,m+1}}{m!\,m}\left(1 + \chi_i + \chi_i^2 + ...\right) \right) = 1$$

Сумма бесконечной геометрической прогрессии $\left(1 + \chi_i + \chi_i^2 + ...\right)$ будет конечной величиной при условии $\chi_i < 1$. Отсюда следует, что число конвейеров m_i в i-м узле следует выбирать как минимальное целое число, удовлетворяющее условию $m_i > \frac{\lambda_i}{\mu_i} \quad \forall i = \overline{1, K}$, иначе сеть не справится с заданным входящим потоком пакетов. Возвращаясь к $P_i(0)$, получаем

$$P_i(0) = \left(\sum_{n=0}^{m} \frac{\rho_i^{\,n}}{n!} + \frac{\rho_i^{\,m+1}}{m!\,m(1-\chi_i)} \right)^{-1} \quad \forall i = \overline{1, K}, \text{ где } m \text{ –}$$

число конвейеров в i-м узле.

Обозначим как $r_i(n)$ длину очереди в *i*-м узле, находящемся в состоянии S_n. В общем виде: $r_i(n) = \begin{cases} 0, n \le m \\ n - m, n > m \end{cases}$, где m – число конвейеров в *i*-м узле.

Средняя длина очереди r_i в *i*-м узле находится как математическое ожидание $r_i(n)$:

$$r_i = \sum_{n=0}^{\infty} r_i(n) P_i(n) = P_i(0) \frac{\lambda_i^{m+1}}{m!\, m \mu_i^{m+1}} \left(1 + 2\frac{\lambda_i}{m\mu_i} + \right.$$

$$\left. + 3\frac{\lambda_i^{\,2}}{m^2 \mu_i^{\,2}} + ... \right) = P_i(0) \frac{\rho_i^{m+1}}{m!\, m} \left(1 + 2\chi_i + 3\chi_i^2 + ...\right)$$

Здесь сумма прогрессии $\left(1 + 2\chi_i + 3\chi_i^2 + ...\right)$ является производной по χ_i суммы прогрессии $\left(\chi_i + \chi_i^2 + ...\right)$, откуда следует:

$$r_i = P_i(0) \frac{\rho_i^{m+1}}{m!\, m (1 - \chi_i)^2} \qquad \forall i = \overline{1, K},$$ где m – число конвейеров в *i*-м узле.

Обозначим как $k_i(n)$ число работающих (обрабатывающих пакеты) конвейеров в *i*-м узле, находящемся в состоянии S_n.

В общем виде:

$k_i(n) = \begin{cases} n, n \le m \\ m, n > m \end{cases}$, где m – число конвейеров в *i*-м узле.

Среднее число работающих каналов k_i в *i*-м узле находит-

ся как математическое ожидание $k_i(n)$:

$$k_i = \sum_{n=0}^{\infty} k_i(n) P_i(n) = P_i(0) \frac{\lambda_i}{\mu_i} \times \left(1 + 2 \frac{\lambda_i}{2! \, \mu_i} + 3 \frac{{\lambda_i}^2}{3! \, {\mu_i}^2} + \ldots \right.$$

$$\left. \ldots + m \frac{{\lambda_i}^{m-1}}{m! \, {\mu_i}^{m-1}} + m \frac{{\lambda_i}^m}{m! \, m {\mu_i}^m} + m \frac{{\lambda_i}^{m+1}}{m! \, m^2 {\mu_i}^{m+1}} + \ldots \right) =$$

$$= P_i(0) \rho_i \left(1 + \rho_i + \frac{{\rho_i}^2}{2!} + \ldots + \frac{{\rho_i}^m}{m!} + \frac{{\rho_i}^{m+1}}{m! \, m} \left(1 + \chi_i + \chi_i^2 + \ldots \right) \right) =$$

$$= P_i(0) \rho_i \left(\sum_{n=0}^{m} \frac{{\rho_i}^n}{n!} + \frac{{\rho_i}^{m+1}}{m! \, m (1 - \chi_i)} \right)^{-1} = \rho_i$$

Получаем $k_i = \rho_i \quad \forall i = \overline{1, K}$.

Среднее число пакетов в *i*-м узле находится как сумма среднего числа работающих каналов и средней длины очереди: $L_i = k_i + r_i \quad \forall i = \overline{1, K}$.

Среднее время пребывания пакета в *i*-м узле находится по теореме Литтла: $T_i = \frac{L_i}{\lambda_i} \quad \forall i = \overline{1, K}$.

Среднее число циркулирующих в сети пакетов $N = \sum_{i=1}^{K} L_i$.

Среднее время пребывания пакета в сети $T = \frac{N}{\sum_{i=1}^{K} \lambda_i}$.

Алгоритм расчета локальных характеристик незамкнутой сети

Шаг 1. Задать начальные условия:

1) λ_0 - интенсивность входящего в сеть потока пакетов;

2) маршрутную матрицу P_R;

3) количество обрабатывающих конвейеров в каждом узле: m_1, m_2, m_3, m_4, m_5, m_6, m_7;

4) средняя интенсивность обработки пакета в одном конвейере каждого узла: $\mu_1, \mu_2, \mu_3, \mu_4, \mu_5, \mu_6, \mu_7$.

Шаг 2. Получить систему линейных уравнений (7) в матричной форме.

Шаг 3. Применить метод Гаусса к (8), чтобы найти передаточные коэффициенты $e_1, e_2, \ldots, e_K$.

Шаг 4. Найти интенсивности потока пакетов, поступающих в каждый узел: $\lambda_i = e_i \lambda_0 \quad \forall i = \overline{1, K}$.

Шаг 5. Найти число конвейеров m_i - минимальное целое число, удовлетворяющее условию $m_i > \dfrac{\lambda_i}{\mu_i} \quad \forall i = \overline{1, K}$.

Шаг 6. Рассчитать вероятности $P_i(0)$:

$$P_i(0) = \left(\sum_{n=0}^{m} \frac{\rho_i^{\,n}}{n!} + \frac{\rho_i^{\,m+1}}{m!\, m(1-\chi_i)} \right)^{-1} \quad \forall i = \overline{1, K}.$$

На последующих шагах алгоритма необходимо найти:

Шаг 7. загруженности каждого узла по формуле: $\chi_i = \dfrac{\lambda_i}{m\mu_i}$ и среднюю загруженность сети.

Шаг 8. среднюю длину очереди в каждом узле:

$$r_i = P_i(0)\frac{\rho_i^{m+1}}{m!\,m(1-\chi_i)^2} \quad \forall i = \overline{1, K}.$$

Шаг 9. среднее число работающих каналов в каждом узле.

Шаг 10. по теореме Литтла рассчитать среднее время пребывания пакета в *i*-м узле: $T_i = \frac{L_i}{\lambda_i} \quad \forall i = \overline{1, K}$.

Шаг 11. среднее число циркулирующих в сети пакетов $N = \sum_{i=1}^{K} L_i$.

Шаг 12. среднее время пребывания пакета в сети $T = \frac{N}{\sum_{i=1}^{K} \lambda_i}$. Конец алгоритма.

В рамках рассматриваемой модели КС (рис. 3) имеет следующие характеристики:

1) $K = 7$ – количество СМО.

2) $\lambda_0 = 3$ – интенсивность входящего в сеть потока пакетов;

3) $P_R = \begin{pmatrix} 0 & 0{,}1 & 0{,}2 & 0{,}3 & 0{,}1 & 0{,}1 & 0{,}1 & 0{,}1 \\ 0{,}1 & 0{,}2 & 0 & 0{,}1 & 0{,}2 & 0{,}1 & 0{,}2 & 0{,}1 \\ 0{,}2 & 0{,}1 & 0{,}1 & 0{,}1 & 0{,}1 & 0{,}2 & 0{,}1 & 0{,}1 \\ 0{,}1 & 0{,}3 & 0{,}1 & 0{,}3 & 0 & 0{,}1 & 0 & 0{,}1 \\ 0{,}1 & 0{,}2 & 0 & 0{,}1 & 0{,}1 & 0{,}2 & 0{,}1 & 0{,}2 \\ 0{,}1 & 0{,}3 & 0{,}1 & 0{,}1 & 0{,}1 & 0{,}1 & 0{,}1 & 0{,}1 \\ 0{,}1 & 0{,}2 & 0{,}2 & 0 & 0{,}1 & 0{,}1 & 0{,}2 & 0{,}1 \\ 0 & 0{,}3 & 0{,}2 & 0 & 0{,}1 & 0{,}1 & 0{,}2 & 0{,}1 \end{pmatrix}$ -

маршрутная матрица.

4) $m_1 = 1$; $m_2 = 1$; $m_3 = 1$; $m_4 = 1$; $m_5 = 1$; $m_6 = 1$; $m_7 = 1$ – количество обрабатывающих конвейеров в каждом узле.

5) $\mu_1 = 45$; $\mu_2 = 45$; $\mu_3 = 30$; $\mu_4 = 30$; $\mu_5 = 15$; $\mu_6 = 15$; $\mu_7 = 50$ – средняя интенсивность обработки пакета в одном конвейере каждого узла.

С целью выявления влияния вредоносных и антивирусных программ на локальные характеристики открытой сети были проведены следующие мероприятия:

1. Моделирование сети в условиях отсутствия вредоносных и антивирусных программ (таблица 6).

Таблица 6 - Характеристики сети в условиях отсутствия вредоносных и антивирусных программ

Номер узла	Загруженность узла, %	Средняя длина очереди, пакеты	Среднее время обработки, ед. вр.
1	15,985	0,030	0,026
2	7,480	0,006	0,024
3	12,980	0,019	0,038
4	12,211	0,017	0,038
5	26,909	0,099	0,091
6	29,876	0,127	0,095
7	7,399	0,006	0,022

2. Моделирование сети под воздействием только вредоносных программ (таблица 7) при $\lambda_0 = 9$. Интенсивность входящего в сеть потока пакетов увеличили в 3 раза для имитации

атаки на сеть.

Таблица 7 - Характеристики сети под воздействием только вредоносных программ

Номер узла	Загруженность узла, %	Средняя длина очереди, пакеты	Среднее время обработки, ед. вр.
1	47,955	0,442	0,043
2	22,439	0,065	0,029
3	38,941	0,248	0,055
4	36,633	0,212	0,053
5	80,726	3,381	0,346
6	89,628	7,745	0,643
7	22,198	0,063	0,026

3. Моделирование сети под воздействием только антивирусных программ (таблица 8). Положим, что производительность конвейеров, вследствие работы антивирусов, снижается на 20%, то есть уменьшается средняя интенсивность обработки пакета в конвейере. Поэтому изменили среднюю интенсивность обработки в конвейере трех из семи узлов: $\mu_1 = 45;\ \mu_2 = 45;\ \mu_3 = 30;\ \mu_4 = 30;\ \mu_5 = 12;\ \mu_6 = 12;\ \mu_7 = 40$.

Таблица 8 - Характеристики под воздействием только антивирусных программ

Номер узла	Загруженность узла, %	Средняя длина очереди, пакеты	Среднее время обработки, ед. вр.
1	19,981	0,050	0,035
2	9,350	0,010	0,031
3	12,980	0,019	0,038
4	12,211	0,017	0,038
5	33,636	0,170	0,126
6	37,345	0,223	0,133

7	9,249	0,009	0,028

Таким образом, средняя длина очереди:

– в условиях отсутствия вредоносных и антивирусных программ: 0,043 пакета;

– под воздействием только вредоносных программ: 1,737 пакета;

– под воздействием только антивирусных программ: 0,071 пакета.

Следовательно, под воздействием вредоносных программ средняя длина очереди в рассматриваемой сети увеличилось в 40,39 раз, а под воздействием АПО – на 65,11% (рис. 6).

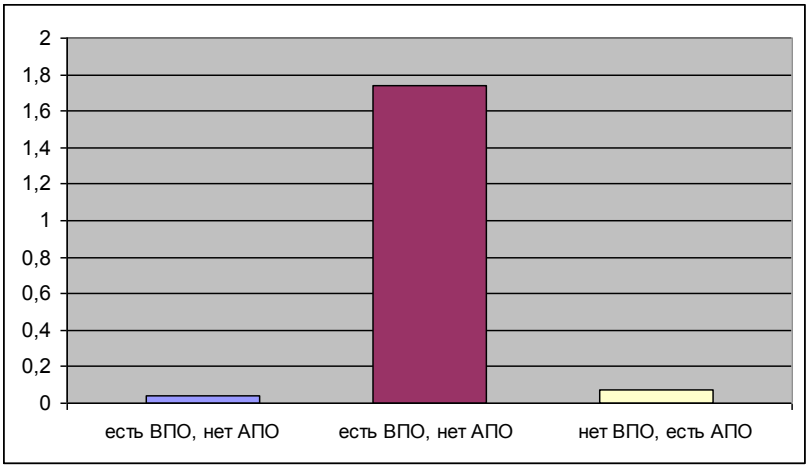

Рисунок 6 - Средняя длины очереди

Среднее время обработки запроса в узле:

– в условиях отсутствия вредоносных и антивирусных программ: 0,047 условных единиц времени;

– под воздействием только вредоносных программ: 0,171 условных единиц времени;

– под воздействием только антивирусных программ: 0,061

условных единиц времени.

Следовательно, под воздействием ВП среднее время обработки запроса в рассматриваемой сети увеличилось на 263,8 %, а под воздействием АПО – на 29,8 %. (рис. 7).

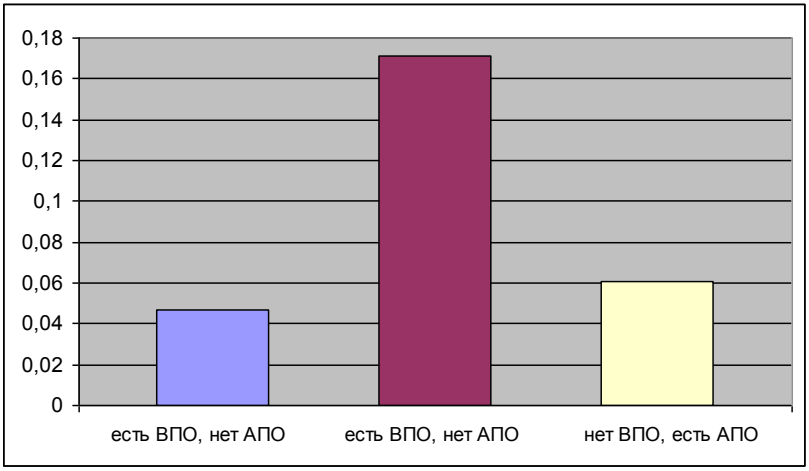

Рисунок 7 - Среднее времени обработки запроса

Согласно анализу данных, полученных в результате изучения состояния сети под воздействием только вредоносных программ, стохастический характер маршрутной матрицы, описывающей сеть, может стать причиной нелинейного роста основных характеристик в некоторых узлах сети, несмотря на то, что загрузка узлов сети будет расти линейно. Такое явление может приводить к сбоям в работе компьютерной сети.

Анализ характеристик рассматриваемой сети под воздействием только АПО показывает, что вследствие запуска антивирусной программы в узлах сети с достаточно высокой средней загруженностью конвейеров, основные характеристики могут ухудшиться в разы.

По результатам сравнения характеристик вычислительной

сети во всех рассмотренных состояниях сделан вывод о том, что наиболее негативно на характеристиках сети сказывается атака вредоносными программами. Однако и действие антивирусов также значительно повышает основные характеристики сети.

Контрольные вопросы и задания

1. Проведите аналитический расчет характеристик реальной замкнутой компьютерной сети.
2. Проведите аналитический расчет характеристик реальной незамкнутой компьютерной сети.
3. Разработайте программу, реализующую алгоритм расчета локальных характеристик замкнутой сети. Результаты работы программы должны быть представлены в табличном виде с графическими иллюстрациями.
4. Разработайте программу, реализующую алгоритм расчета локальных характеристик незамкнутой сети. Результаты работы программы должны быть представлены в табличном виде с графическими иллюстрациями.
5. Разработайте программу для определения минимального количества обслуживающих устройств в узлах сети для разного входящего потока пакетов. Компьютерная сеть должна при любых условиях быть работоспособной и эффективной в обслуживаний.

Глава 3. Имитационные модели компьютерной сети

Аналитические методы весьма стеснительны для решения практических задач: например, выдвигается предположение о простейшем потоке заявок (для разных фаз обслуживания он может быть не простейшим), однотипных устройствах и т.д.

В имитационном моделировании (ИМ) все ограничения снимаются (например, могут использоваться произвольные законы распределения для описания временных параметров, различные схемы (порядок обслуживания) и т.д.), объекты исследуется не обязательно в стационарном режиме (например, возможно изучение переходного режима, когда показатели отличаются от асимптотических значений).

Сущность метода имитационного моделирования для СМО: используются специальные алгоритмы, позволяющие вырабатывать случайные реализации потоков событий и моделировать процессы функционирования обслуживающих систем. Далее осуществляется многократное воспроизведение, реализация случайных процессов обслуживания и статистическая обработка на выходе - оценка показателей качества обслуживания.

Имитационное моделирование позволяет решать ряд сложных задач и имеет следующие преимущества:

– при создании имитационной модели законы функционирования системы могут быть неизвестны, поэтому постановка задачи исследования является не полной и ИМ служит средством изучения особенностей процесса. При этом можно руководствоваться связями между компонентами и алгоритмами их поведения;

– при проведении ИМ выявляется характер связей между внутренними параметрами системы и выходными характеристиками;

– при проведении ИМ можно менять темп моделирования: ускорять при моделировании явлений макромира (например, процессов на Солнце) или замедлять при моделировании явлений микромира (например, процесс существования элементарных частиц).

Из перечисленного следует, что ИМ применяется для решения широкого спектра задач практически любой сложности в условиях неопределенности, когда аналитическое моделирование оказывается практически не применимым.

Достоинства имитационного моделирования

1. Возможность объединять традиционные математические и экспериментальные компьютерные методы.

2. Высокая эффективность применения при исследовании АСНИ, САПР, экспертных систем, сложных систем управления. По данным RAND Corp., консалтинговые фирмы из всей гаммы возможных средств анализа: линейного, нелинейного, динамического программирования, методов исследования операций, вычислительных методов - более чем в 60 % случаев прибегают к ИМ, так как ИМ позволяет получать ответы в терминах, понятных и привычных для пользователя.

3. Возможность исследовать объекты, физическое моделирование которых экономически нецелесообразно или невозможно.

4. Исследование еще не существующих объектов.

5. Исследование труднодоступных или ненаблюдаемых объектов.

6. Исследование плохо формализуемых экологических, социальных или экономических систем.

7. Исследование объектов практически любой сложности при большой детализации и снятии ограничений на вид функций распределения случайных величин.

Недостатки имитационного моделирования

1. Самым существенным недостатком является невозможность получить точечную оценку исследуемых характеристик, так как в результате ИМ можно оценить только математическое ожидание и дисперсию.

2. Потеря общности результатов, так как при имитационном моделировании оценивается конкретная система.

3. Трудности с оценкой адекватности имитационных моделей.

4. Создание ИМ сложной системы длительно по времени и требует значительных денежных средств.

Несмотря на эти недостатки, все большее число исследователей прибегает к использованию ИМ в силу его достоинств. Для составления достаточно сложной имитационной модели необходимы опыт и приобретаемые на практике навыки. Это следует учитывать, чтобы при первых неудачах не наступило разочарование в возможностях ИМ.

3.1 Система имитационного моделирования GPSS World

Имитационное моделирование объединяет достижения математического моделирования, системного программирования и информационных технологий. ИМ обладает:

– способностью понимать, интерпретировать и использовать формализованную и не формализованную информацию (математические формулы, логические правила, вербальные описания и т. п.);

– различными формами представления данных и знаний, заполняя пространство между математическими моделями с его аналитическими формами описания и искусственным интеллектом с его формами и правилами представления знаний;

– способностью участвовать в процессе не только автоматизации научных исследований за счет использования самой ЭВМ для модификации различных режимов применения КМ, но и интеграции всех этапов жизненного цикла системы путем использования быстро развивающихся методов ИТ (широко распространенные во всем мире CALS-технологии, CASE-технологии, технологии ICAM и IDEF);

– возможностью расширения круга пользователей, от узкого круга специалистов-математиков и профессиональных программистов до большого класса исследователей, не обладающих профессиональными знаниями в областях математики и программирования, но хорошо знающих предметную область и умеющих обращаться с ППП.

В мире информационных технологий имитационное моделирование переживает вторжение рождение. И это в первую очередь связано с появлением в 2000 году мощного программного продукта фирмы Minuteman Software – GPSS World (GPSSW, General Purpose System Simulation Word – Мировая общецелевая система моделирования), разработанного для ОС Windows. Этот программный продукт вобрал в себя арсенал новейших информационных технологий. Он включает развитые графические оболочки для создания моделей и интерпретации выходных результатов моделирования, мультимедийные средства и видео, объектно-ориентированное программирование и др. В основу системы GPSS World положен язык GPSS, разработанный профессором Гордоном в 60-х годах 20 века. В такой бурно развивающейся области, как программное обеспечение, только небольшое количество языков программирования достигло подобного почтенного возраста. Долгожительство языка GPSS объясняется многими причинами:

– он прост в изучении и использовании;

– наиболее важные классы объектов (требования (транзакты), каналы, накопители, логические переключатели и др.) и их свойства широко используются в реальных вычислительных сетях, производственных и коммерческих системах и т.д.;

– диапазон использования языка достаточно широк;

– язык постоянно совершенствуется;

– расширение создаваемых моделей легко осуществимо;

– достаточно широкое использование анимации;

– пользователи способны легко понять внутреннюю логику и алгоритмы GPSS;

– интерфейс прост и удобен;

– при построении модели язык позволяет оперировать непосредственно понятиями имитируемой системы.

Система GPSS World – мощная универсальная среда моделирования как дискретных, так и непрерывных процессов, предназначенная для профессионального моделирования самых разнообразных процессов и систем.

GPSS World является объектно-ориентированным языком. В совокупность его основных объектов входят объекты «Модель», используемые для создания объектов «Процесс моделирования». Объекты «Процесс моделирования» в свою очередь используются для осуществления процесса моделирования и создания объектов «Отчет».

GPSSW обеспечивает автоматическое составление подробных статистических стандартных отчетов, которые, как правило, содержат достаточные для анализа выходные статистические данные о конечных состояниях всех традиционных объектов GPSS.

С помощью системы GPSS World возможно произвести оценку показателей качества обслуживания КС:

– общее количество обслуженных заявок, за какой- либо промежуток времени;

– пропускная способность (среднее число заявок, обслуженных в единицу времени);

– доля заявок обслуженных;

– доля заявок, получивших отказ;

– время пребывания заявки в системе (от момента поступления заявки в систему до момента завершения ее обслуживания);

– среднее время обслуживания (функция распределения времени обслуживания);

– средняя длина очереди;

– среднее время ожидания;

– загрузка каналов - коэффициент использования (как доля времени, в течение которого ОУ было занято) – характеризует степень простоя ОУ.

3.2 Имитационная модель компьютерной сети в GPSS World

Объект изучения – компьютерная сеть предприятия Гос. НИИЛЦ РФ «Радуга» на 13 производственной площадке.

В состав компьютерной сети входят следующие технические средства: 4 рабочих станций, 1 сервера, 1 сетевого коммутатора, объединенных сетевыми кабелями. Имеется связь с внешней локальной сетью и сетью Интернет. Топология сети представлена на рис. 1. В таблице 1 представлена конфигурация сетевых устройств, в таблице 2 – устройства, подключаемые к сети, в таблице 3 – профили приложений узлов компьютерной сети.

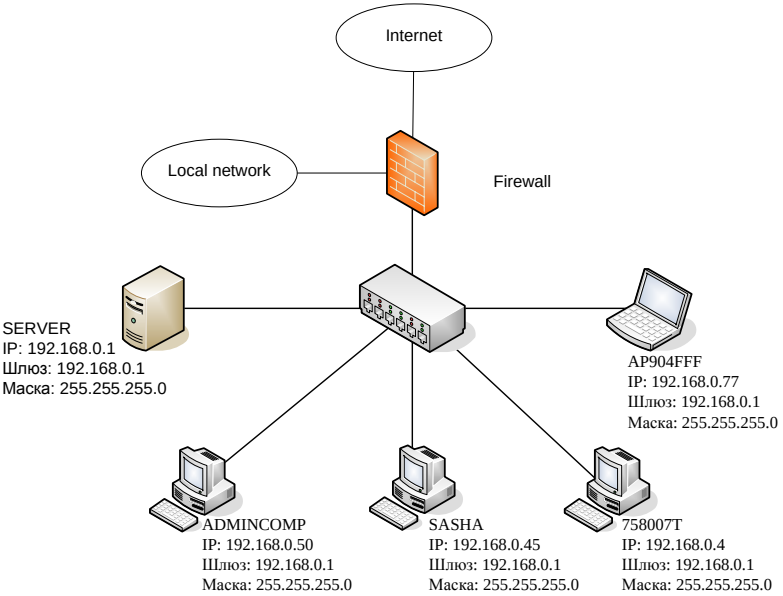

Рисунок 1 – Структура компьютерной сети

Таблица 1 – Конфигурация сетевых устройств

Условное обозначение	Модель	Интерфейс	Параметры
Hub	Compex RS2208B	8-Port 10/100Mbps Fast Ethernet	Количество портов: 8; Скорость передачи данных – 10/100 Мбит/с; Half/Full duplex на всех портах; Авт. переключение MDI/MDIX – да;

Блок питания – внешний.

Таблица 2 - Устройства, подключаемые к сети

Имя Устройства IP-адрес/маска подсети	Платформа ОС	Интерфейс	Службы
Server 192.168.0.1/24	Linux	10/100Mbps Fast Ethernet	Inetd, ssh, ras (FTP-сервер), samba (файл-сервер), named (DNS-сервер), postfix (SMTP-сервер), dovecot (pop3-сервер), Apach 2 (web-сервер), ssl, MySQL (СУБД-сервер), socks5
AP904FFF 192.168.0.77/24			1С Предприятие 7.7, MS Office 2007, Adobe Reader 8, 7-Zip 4.44 Beta, FarManager v 1.70, Антиви-
Admincomp 192.168.0.50/24	Windows XP SP2		
SASHA 192.168.0.45/24			

```
758007T                          рус Касперско-
192.168.0.4                      го 7.0 (или
/24                              Dr.Web 4.44
                                 или Avast! 4
                                 Home Edition),
                                 MS Internet
                                 Explorer 9.0,
                                 Opera 9.24
```

Таблица 3 – Профили приложений

Название профиля	Программный продукт	Требования к сети
MS Office	Microsoft Office Enterprise 2007 RUS	Периодический обмен с сервером (файловый сервер). Достаточная скорость - 10 Мбит/с. Основные порты: 20, 21.
Антивирусные системы	Dr.Web 4.44	Периодический обмен с сервером обновления. Достаточная скорость - 10 Мбит/с. Основные порты: 80.
	Антивирус Касперского 7.0	– // – // – // – // – // –
	Avast! 4 Home Edition	– // – // – // – // – // –
Браузеры	MS Internet Explorer 9.0	Периодический обмен с различными сетевыми хостами. Достаточная скорость - 10 Мбит/с. Основные порты: 80, 8080, 443.

	Opera 9.24	Периодический обмен с различными сетевыми хостами. Достаточная скорость - 10 Мбит/с. Основные порты: 80, 8080, 443.
1С	1С: Предприятие 7.7 (сетевая версия)	Постоянный обмен с сервером 1С. Достаточная скорость - 100 Мбит/с. Основные порты: 425, 441, 137-139.
Специальные приложения	MySQL (СУБД-сервер)	Постоянный обмен с сервером. Достаточная скорость - 100 Мбит/с. Основные порты: 3306.
	7 Zip	Периодический обмен с сервером. Достаточная скорость - 100 Мбит/с. Основные порты: 137-139.

Постановка задачи

Исследовать влияние вредоносных и антивирусных программ на характеристики КС с помощью системы имитационного моделирования GPSS World.

Работа КС формализуется в виде СМО с ограниченной очередью. Поток заявок распределен по закону Пуассона с интенсивностью λ заявок на ед.вр. (увеличивается при воздействии ВП), а время обработки заявки распределено экспоненциально, интенсивность обработки - μ (увеличивается при воздействии АП).

Характеристики СМО:

– среднее количество пакетов (заявок) в очереди;

– общее число пакетов (заявок) в очереди, то есть запросов ожидавших момента обслуживания в течении работы системы;

– средняя продолжительность пребывания заявки в системе.

Требуется: провести сравнительный анализ характеристик КС в условиях работы вредоносных и антивирусных программ.

Формализация задачи

Моделируемый процесс: передача пакетов (заявок) от рабочих станций пользователей к серверу КС. При построении модели определены следующие базовые параметры системы:

1) Единица времени в моделируемой системе - 1 секунда. Размер передаваемого пакета в моделируемой системе: 100 Мбайт.

2) Пропускная способность канала связи: 100 Мбит/с. Исходя из этого задержка на передачу пакета по каналу связи равна 8 секунд.

3) Количество рабочих станций - 4. Станции генерируют пакеты для отправки по каналу связи обрабатывающему серверу (таблица 3). Количество обрабатывающих каналов сервера - 3. Пакеты, поступают в один из свободных каналов на обработку.

Таблица 3. Средние интервалы времени генерации пакетов рабочими станциями

Рабочая станция	Интервал времени, сек.
PC1	23 ± 3
PC2	30 ± 2
PC3	25 ± 4
PC4	40 ± 6

4) Ёмкости накопителя пакетов, поступивших на обработ-

ку – 5. Если все обрабатывающие каналы заняты, то пакеты встают в очередь на обработку. Если очередь заполнена, то пришедший пакет получает отказ в обслуживании.

5) Время обработки пакета в ЦП сервера — 110 секунд. После обработки пакет выходит из системы.

Определены изменения параметров СМО при моделировании воздействия ВП на характеристики КС:

1) Количество генерируемых пакетов увеличивается на 69% (таблица 4).

Таблица 4. Средние интервалы времени генерации пакетов рабочими станциями с повышенной частотой генерации

Рабочая станция	Интервал времени, сек.
PC1	7,13 ± 1
PC2	9,3 ± 0,6
PC3	7,75 ± 1,25
PC4	12,4 ± 1,85

2) Задержка на обработку пакетов сервером увеличивается на 75%. Время обработки пакета в ЦП сервера с учётом данного влияния равна 192,5 секунды.

3) Возможность доступа пакетов к серверу уменьшается на 18%. Ёмкость накопителя пакетов с учётом данного влияния – 4.

При моделировании воздействия АП на характеристики КС рассматривались три продукта: Антивирус Касперского 7.0; Dr.Web 4.44; Avast! 4 Home Edition.

Определены изменения параметров моделируемой системы под воздействием АП (таблица 5): ухудшается пропускная способность канала (задержка на передачу пакета по каналу связи увеличивается), уменьшается производительность системы (задержка на обработку пакетов сервером увеличивается).

Таблица 5. Изменение параметров моделируемой системы под

воздействием АП

	Задержка на обработку пактов, сек	Ухудшение пропускной способности канала связи, %	Задержка на передачу пакетов, сек.
Антивирус Касперского 7.0	152,75	12,6	9
Dr.Web 4.44	140,5	5,15	8,4
Avast! 4 Home Edition	170	4,4	8,35

Моделирование системы

Процесс моделирования системы облегчает построение графической схемы имитационной модели (рис. 2). Графическая схема отображает логику взаимодействия блоков имитационной модели.

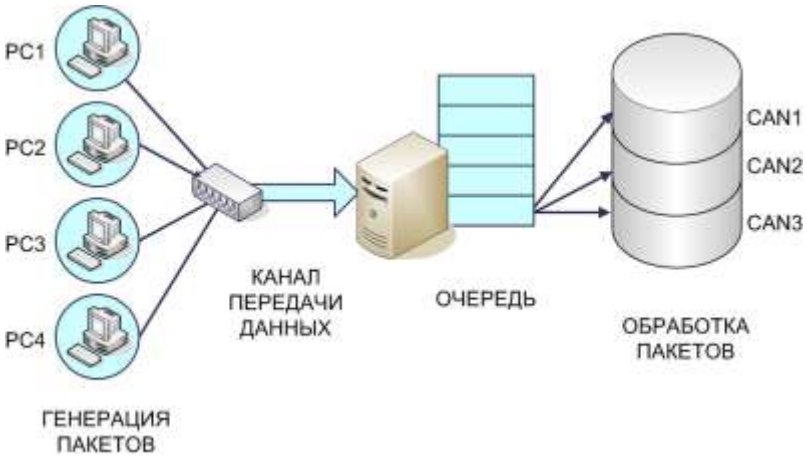

Рисунок 2 - Схема функционирования имитационной модели

Прогон модели с разными входными данными в среде GPSS World позволяет получить статистические результаты,

которые выводятся в виде стандартных отчётов и могут быть представлены графически в виде графиков и гистограмм.

Для решения поставленной задачи были проведены следующие мероприятия:

1) Исследование работы моделируемой системы в условиях отсутствия вредоносных и антивирусных программ.

2) Исследование работы моделируемой системы при воздействии вредоносных программ.

3) Исследование работы моделируемой системы при воздействии антивирусных программ.

В отчеты экспериментов (рис. 3) включены основные показатели моделирования системы:

1) О каналах обрабатывающего устройства (FACILITY) с условными именами CAN1, CAN2 и CAN3:

– ENTIRES - количество пакетов, прошедших через устройство;

– UTIL - коэффициент использования устройства;

– AVE._TIME - среднее время обработки одного пакета в устройстве;

– AVAIL – состояние готовности устройства в конце периода моделирования;

– OWNER - номер последнего пакета, занимавшего устройство;

– PEND - количество пакетов, ожидающих устройство, находящееся в режиме прерывания

– INTER - количество пакетов, прерывающих устройство в данный момент;

– RETRY - количество пакетов, ожидающих специальных условий, зависящих от состояния устройства;

– DELAY - количество пакетов, ожидающих занятия или освобождения устройства.

2) Об очереди (QUEUE) заявок на обработку с уловным именем LINE1:

– MAX - максимальное содержимое очереди в течение периода моделирования;

– CONT - текущее содержимое очереди в конце периода моделирования;

– ENTRIES - общее количество входов в накопитель;

– ENTRIES(0) - общее количество входов в очередь с нулевым временем ожидания;

– AVE.CONT - среднее значение содержимого очереди;

– AVE.TIME - среднее время, проведенное в очереди с учетом всех входов в очередь;

– AVE.(-0) - среднее время, проведенное в очереди без учета «нулевых» входов в очередь;

– ETRY - количество транзактов, ожидающих специальных условий, зависящих от состояния очереди;

На рис. 4 – 12 представлены гистограммы результатов моделирования, где Mean – среднее значение исследуемого параметра; S.D. – среднее квадратическое отклонение.

Моделирование сети в условиях отсутствия вредоносных и антивирусных программ

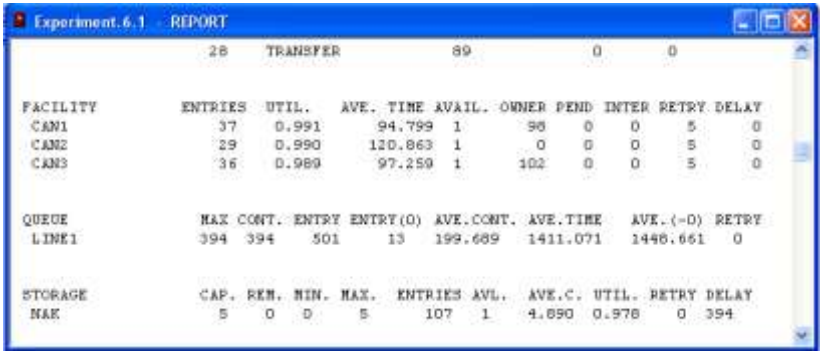

Рисунок 3 Вывод результатов моделирования

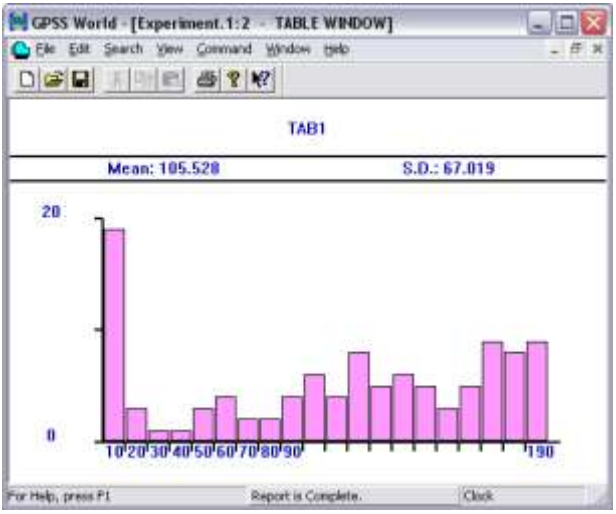

Рисунок 4 – Среднее количество пакетов в очереди

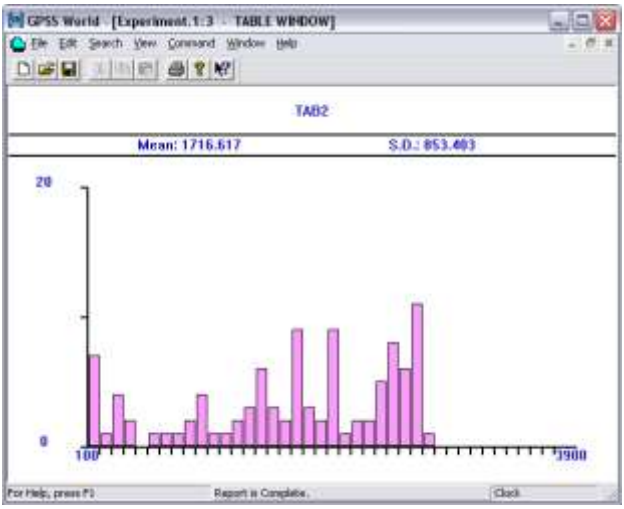

Рисунок 5 – Средняя продолжительность пребывания пакета в системе

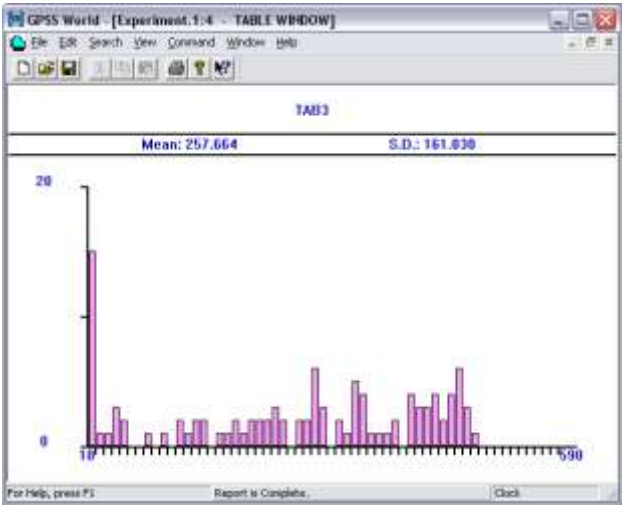

Рисунок 6 – Число пакетов ожидавших момента обслуживания

Моделирование сети под воздействием ВПО

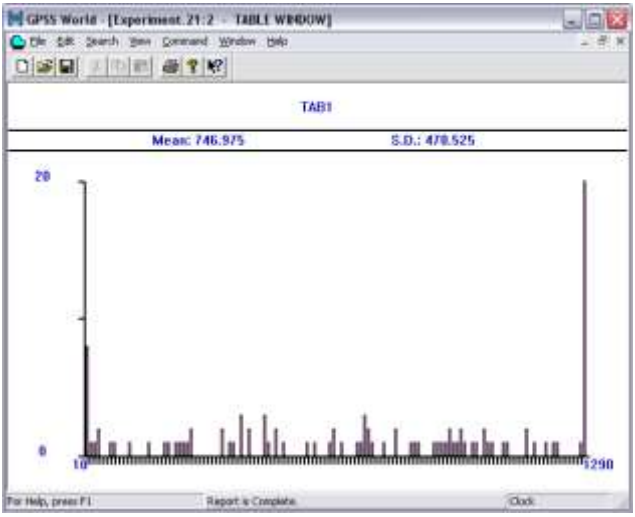

Рисунок 7 – Среднее количество пакетов в очереди

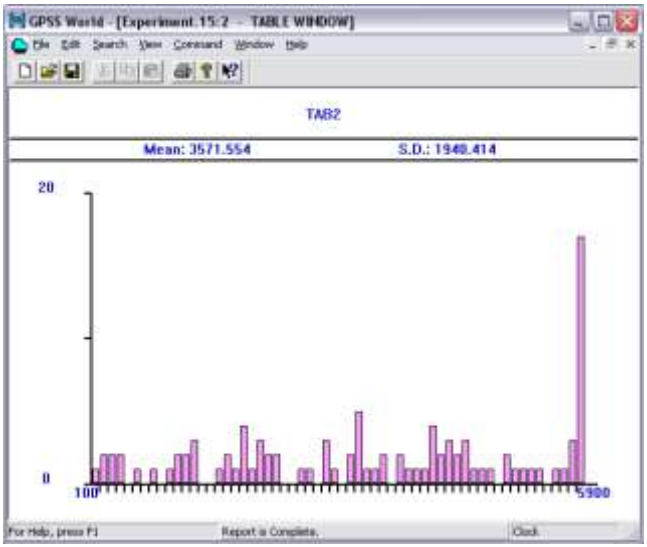

Рисунок 8 – Средняя продолжительность пребывания пакета в системе

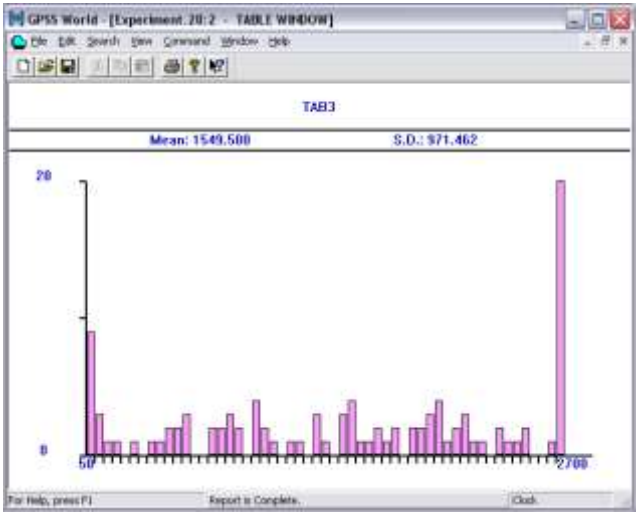

Рисунок 9 – Число пакетов ожидавших момента обслуживания

Моделирование сети под воздействием только антивирусных программ

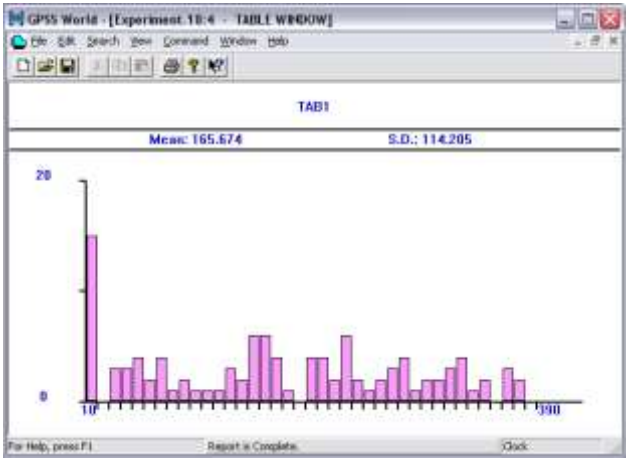

Рисунок 10 – Среднее количество пакетов в очереди

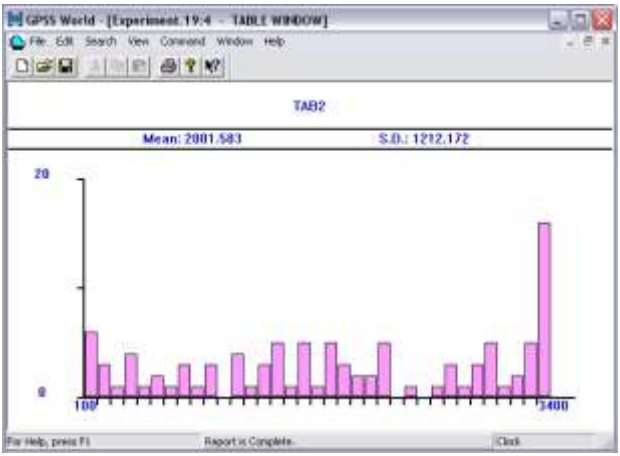

Рисунок 11 – Средняя продолжительность пребывания пакета в системе

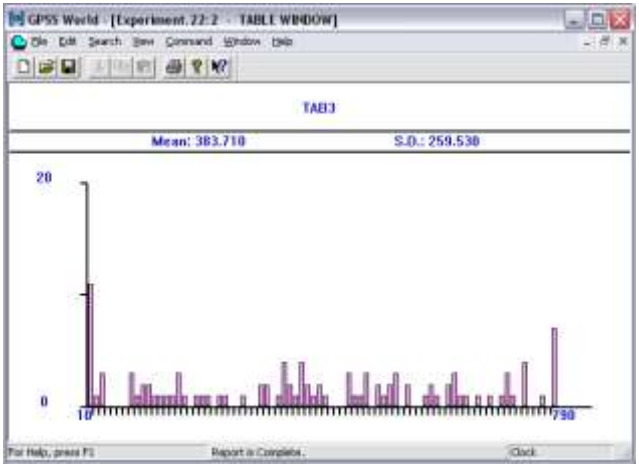

Рисунок 12 – Число пакетов ожидавших момента обслуживания

Графическое представление результатов моделирование визуально отображает увеличение загрузки канала связи и увеличении времени пребывания пакета в системе.

Средние значения характеристик КС по проведенным экс-

периментам представлены в таблице 6.

Таблица 6. Средние значения характеристик КС

Эксперимент	Среднее количество пакетов в очереди	Средняя продолжительность пребывания пакета в КС, ед.вр.	Общее число пакетов ожидавших момента обслуживания
Без влияния	105,8	1716,617	257,664
Влияние ВП	746,975	3571,554	1549,5
Влияние АП	165,674	2001,583	383,710

Имитационное моделирование позволило количественно оценить воздействие вредоносных и антивирусных программ на характеристики корпоративной сети. Наиболее негативно на характеристиках сети оказывают вредоносные программы (увеличивают частоту генерации пакетов, что перегружает очередь). Однако и действие антивирусных средств также значительно ухудшает основные характеристики сети (АП увеличивают задержку пакетов в системе, что замедляет обработку потока пакетов по времени).

Исследование доказывает, что при развертывании систем защиты на предприятиях необходимо учитывать, что системы призваны обеспечить не только максимальную защищенность информационных ресурсов, но и не ухудшить системные характеристики КС.

Контрольные вопросы и задания

6. Проведите сравнительный анализ различных языков имитационного моделирования. Выявите достоинства и недостатки. Сделайте вывод

о целесообразности практического применения каждого из них.

7. Постройте имитационную модель реальной компьютерной сети в среде GPSS World.
8. Проведите исследование аналитической и имитационной модели реальной компьютерной сети в условиях воздействия вредоносных программ. Сравните полученные результаты.
9. Проведите исследование аналитической и имитационной модели реальной компьютерной сети в условиях воздействия антивирусных программ. Сравните полученные результаты.
10. С помощью имитационного модели реальной компьютерной сети выберите средства противодействия вредоносным программам, способные обеспечить максимальную защиту без нарушения работоспособности и эффективности системы.

Заключение

Настоящее учебное пособие дает базовые знания, необходимые для аналитического и имитационного моделирования компьютерных сетей в условиях воздействия вредоносных программ. В теоретической части пособия систематизирован материал по аналитическому и имитационному моделированию в задачах оценки сетевых характеристик в условиях вредоносного информационного воздействия. Рассмотрен актуальный вопрос количественной оценки влияния вредоносных и антивирусных программ на характеристики компьютерной сети.

В практической части глав учебного пособия представлены примеры аналитического расчета сетевых характеристик в

условиях вредоносного информационного воздействия, имитационные модели компьютерных сетей и графическая иллюстрация полученных результатов. Разработаны контрольные вопросы и задания.

Для получения более глубоких знаний можно обратиться к публикациям, приведенным в библиографическом списке. Тем не менее, авторы полагают, что студенты, изучив теоретические аспекты, изложенные в пособии, готовы к самостоятельному изучению соответствующих вопросов для дальнейшего повышения квалификации.

Авторы выражают глубокую благодарность рецензентам учебного пособия: кандидату технических наук, доценту, зав. кафедрой ОТД Владимирского юридического института ФСИН России К.Н. Курысеву и доктору технических наук, профессору, зав. кафедрой БЖ Владимирского государственного университета О.В.Веселов.

Библиографический список

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов / В. Г. Олифер, Н. А. Олифер. – Питер, 2007. – 960 с. – ISBN 5-469-00504-6.

2. Бройдо, В. Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. / В. Л. Бройдо. – Питер, 2006. – 704 с. – ISBN 5-318-00530-6.

3. Советов, Б.Я. Моделирование систем: Учебное пособие для вузов / Б.Я. Советов, С.А. Яковлев. – М.: Высш.шк., 2001. – 343 с. ISBN 5-06-003860-2.

4. Советов, Б.Я., Моделирование систем: Практикум: Учебное пособие для вузов / Б.Я. Советов, С.А. Яковлев. – М.: Высш.шк., 2003. – 295 с.: ил. – ISBN 5-06-004087-9.

5. Осипов, Л. А. Моделирование информационных процессов: Учебное пособие / Л. А. Осипов. – М.: РГОТУПС, 2005. – 207 с. – ISBN 5-7473-0247-7.

6. Тарасик, В.П. Математическое моделирование технических систем: Учебник для вузов / В.П. Тарасик. – Мн.: ДизайнПРО, 1997.– 640с. – ISBN 985-6182-10-7.

7. Вентцель, А.Д. Курс теории случайных процессов / А.Д. Вентцель. – М.: Наука, 1972. – 320 с.

8. Боровков, А.А. Вероятностные процессы в теории массового обслуживания / А.А. Боровков. – М.: Наука, 1972. – 367 с.

9. Ивченко, Г.И. Теория массового обслуживания / Г.И. Ивченко, В.А. Каштанов, И.Н. Коваленко. – М.: Высшая школа, 1982. – 256 с.

10. Чернов, В.П. Теория массового обслуживания. Учебное пособие / В.П. Чернов, В.Б. Ивановский. – М.: ИНФРА, 2000. – с. – ISBN 5-16-000164-6.

11. Вентцель, Е.С.. Теория случайных процессов и ее инженерные приложения: Учебное пособие для вузов, Изд. 4-е, стереотип. 3-е изд. перераб. и доп. / Е.С. Вентцель, Л.А. Овчаров. – М.: Высшая школа, 2007. – 432 с. – ISBN 978-5-06-005820-8.

12. Шелухин, О. И. Моделирование информационных систем / О. И. Шелухин, А. М. Тенякшев, А. В. Осин. – М.: Радиотехника, 2005. – 368 с. – ISBN 5-93108-072-4.

13. Колбанев, М. О. Модели и методы оценки характеристик обработки информации в интеллектуальных сетях связи (монография) / М. О. Колбанев, С. А. Яковлев. – СПб.: Издательство СПбГУ, 2002. – 230 с. – ISBN 5-288-03061-8.

14. Кутузов, О. И. Имитационное моделирование сетей массового обслуживания. Учебное пособие / О. И Кутузов, В. Н Задорожный, С. И. Олзоева. – Улан-Удэ: Изд-во ВСГТУ, 2001. – 228 с. – ISBN 5-89230-184-2.

15. Рыжиков, Ю.И. Имитационное моделирование. Теория и технологии / Ю.И. Рыжиков. – СПб.: КОРОНА принт, 2004. – 384с. – ISBN 5-94271-021.

16. Шрайбер, Т.Дж. Моделирование на GPSS / Т.Дж. Шрайбер. – М.: Машиностроение, 1980.– 592с.

17. Боев, В.Д. Моделирование систем. Инструментальные средства GPSS World / В.Д. Боев. – СПб.: БХВ-Петербург, 2004. – 368 с. – ISBN 5-94157-515-7.

18. Аверилл, М. Лоу Имитационное моделирование / М. Лоу Аверилл, В. Дэвид Кельтон. – СПб.: Питер, Издательская группа BHV, 2004. – 848 с. – ISBN 5-94723-981-7 .

19. Бражник, А.Н. Имитационное моделирование: возможности GPSS World / А.Н. Бражник. – СПб.: Реноме, 2006. – 439 с. – ISBN 5-98947-036-3.

20. Карпов, Ю.Г. Имитационное моделирование систем. Введение в моделирование с AnyLogic 5 / Ю.Г. Карпов. – СПб.: БХВ-Петербург, 2006. – 400 с. – ISBN 5-94157-148-8.

21. Кудрявцев, Е.М. GPSS World. Основы имитационного моделирования различных систем / Е.М. Кудрявцев. - М.: ДМК Пресс, 2004. – 320 с. – ISBN 5-94074-219.

22. Рыжиков, Ю.И. Имитационное моделирование: Теория и технологии / Ю.И. Рыжиков. – СПб.: КОРОНА принт, 2004. – 384 с. – ISBN 5-94271-021.

23. Шеннон, Р. Дж. Имитационное моделирование систем - искусство и наука / Р. Дж. Шеннон. – М.: Мир, 1978 г. – 418 с.

24. Gordon, Geoffre. System Simulation, 2nd ed., Prentice-Hall, 1978.

25. Harrell, Charles R. and Kerim Tumay. Simulation Made Easy, Industrial Engineering Press, 1995.

26. Hoover, Stewart V. and Ronald F. Perry, Simulation: A Problem Solving Approach, Addisson-Wesley. Reading Massachusetts, 1990.

27. Knepell, Peter L. and Deborah C. Arangno. Simulation Validation, IEEE Computer Society Press, 1993.

28. Law, Averill M. and David W. Kelton. Simulation Modeling and Analysis, McGraw-Hill, 1991.

29. Neelamkavil, Francis Computer Simulation and Modeling, John Wiley & Sons, 1987.

30. Pritsker, Alan B. and Claude Dennis Pegden. Introduction to Simulation and SLAM, John Wiley & Sons, 1979.

31. Beytuk, Yuri. GPSS-simulator of distributed control system in flexible manufacturing (статья). Proc. of the XXXI JUREMA'86, 31st Annual Gathering JUREMA, First symposium on automata and robots in process automatization, 22-25 Apr. 1986, p.p.401-405.

32. Beytuk, Yuri. Estimation of characteristics and optimizing the structure of measuring and controlling contour for flexible technological cell on GPSS-model base (статья). Proc. of Int. Conf. IMEKO'86 "Intelligence measurement", Jena, 10-14 Jun., 1986, p.p.287-293.

33. Carson, J. S., “Convincing User’s of Model’s Validity is Challenging Aspect of Modeler’s Job”, Industrial Engineering, June 1986, p. 77.

34. Law, Averill M. “Designing and Analyzing Simulation Experiments”, Industrial Engineering, March 1991, pp. 20-23.

35. Thesen, Arne and Laurel E. Travis, Simulation For Decision Making, West Publishing Company, 1992.

36. Tomashevskiy V. Automatic generating of GPSS/PC programs. Proceedings 15th European Simulation Multiconference, Prague, 2001.

37. Tumay, Kerim, Business Process Reengineering Using Simulation, Autofact Workshop, 1993.

38. Антивирусная защита компьютерных систем. Методы защиты от вредоносных программ. [Электронный ресурс]. - http://www.intuit.ru/department/security/antiviruskasp/5/

39. Антивирус Касперского 7.0. [Электронный ресурс]. - http://www.kaspersky.ru/kaspersky_anti-virus_7_0

40. Антивирус ESET NOD32 [Электронный ресурс]. - http://www.esetnod32.ru/products/av_home.php

41. Обзор вирусной активности, апрель 2008 [Электронный ресурс].
http://www.viruslist.com/ru/analysis?pubid=204007606

42. Тенденции развития антивирусного рынка [Электронный ресурс]. - http://www.connect.ru/article.asp?id=6201

ОГЛАВЛЕНИЕ