На правах рукописи

МУЛЮХА Владимир Александрович

РАЗГРАНИЧЕНИЕ ДОСТУПА В КОМПЬЮТЕРНЫХ СЕТЯХ НА ОСНОВЕ КЛАССИФИКАЦИИ И ПРИОРИТЕТНОЙ ОБРАБОТКИ ПАКЕТНОГО ТРАФИКА

Специальность 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2010

Работа выполнена в Государственном образовательном учреждении высшего профессионального образования «Санкт-Петербургский государственный политехнический университет»

Научный руководитель:
доктор технических наук,
профессор Заборовский Владимир Сергеевич

Официальные оппоненты:
доктор технических наук,
профессор Хомоненко Анатолий Дмитриевич

кандидат технических наук,
доцент Павлов Александр Николаевич

Ведущая организация:
Институт проблем информационной безопасности Московского государственного университета имени М.В.Ломоносова

Защита состоится «23» декабря 2010 г. в 16 часов на заседании диссертационного совета Д 212.229.27 при ГОУ ВПО «Санкт-Петербургский государственный политехнический университет» по адресу 195251, Санкт-Петербург, ул. Политехническая, 29, ауд. 175 главного здания.

С диссертацией можно ознакомиться в фундаментальной библиотеке ГОУ ВПО «Санкт-Петербургский государственный политехнический университет»

Автореферат разослан «_____» ноября 2010г.

Ученый секретарь диссертационного совета Платонов В.В.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Развитие сетевых технологий в направлении широкого использования интерактивных и мультимедийных приложений предъявляет новые требования к компьютерным сетям (КС) как безопасной среде доступа к распределенным информационным объектам. Традиционные подходы не в полной мере учитывают специфику современных глобальных КС, в которых значительную часть сетевых приложений стали составлять открытые информационные ресурсы, доступ к которым не отвечает требованиям корпоративной политики безопасности. Поэтому, в настоящее время особую актуальность приобретает задача разграничения доступа, учитывающая специфику межсетевого взаимодействия на основе стека протоколов TCP/IP, ограничения на пропускную способность каналов связи и угрозы безопасности со стороны скрытных информационных воздействий.

Сложность решения этой важной научно-технической задачи отмечается как российскими, так и зарубежными учёными, в том числе П.Н. Девяниным, Н.А. Гайдамакиным, П.Д. Зегждой, Л.Дж. Хоффманом и многими другими, что связано с необходимостью разработки эффективных алгоритмов классификации информационных ресурсов и приоритетной обработки данных в процессе коммутации пакетного трафика, отвечающие рекомендациям RFC и требованиям архитектуры DiffServ.

Одним из перспективных путей решения сформулированной выше задачи является формализация процессов межсетевого взаимодействия на основе описания пакетного трафика как совокупности различных классов виртуальных соединений (ВС), используемых для доступа к информационным ресурсам на различных уровнях межсетевого взаимодействия стандартной модели ВОС. В этом случае попытки несанкционированного доступа могут блокироваться с помощью программно-аппаратных средств межсетевого экранирования, функционирующих на основе оперативной классификации ВС и последующей приоритетной обработки трафика с учетом требований к качеству функционирования различных информационных приложений.

В рамках такого подхода необходимо учитывать двойственность задачи разграничения доступа (РД), которая связана с необходимостью блокирования нежелательных удаленных воздействий и одновременным контролем информационного обмена субъектов с открытыми сетевыми ресурсами. Важным аспектом, повышающим эффективность применения систем РД, является необходимость решения задач классификации и приоритетной обработки в реальном масштабе времени, что в свою очередь делает актуальным разработку методов аналитического расчета пропускной способности каналов связи в условиях случайных возмущений, обладающих свойствами статистического самоподобия из-за особенностей реализации современных транспортных протоколов.

При этом в связи с постоянным развитием методов сокрытия данных и отклонениями реализаций сетевых сервисов от рекомендаций RFC, актуальной задачей совершенствования средств РД является динамический контроль допустимого множества состояний ВС, отвечающих информационной модели объекта доступа, на основе которой формулируются требования к корпоративной политике доступа.

С учётом всего вышеизложенного, актуальной научно-технической задачей РД является разработка принципов оперативной классификации сетевых ресурсов, создание моделей описания ВС и средств приоритетной обработки трафика, учитывающих динамические и статистические характеристики потоков данных, формируемых в процессе доступа к информационным ресурсам современных компьютерных сетей.

Целью исследования является разработка метода оперативной классификации и алгоритмов приоритетной обработки пакетного трафика для разграничения доступа в компьютерных сетях с учетом требований безопасности и особенностей реализации современных транспортных протоколов.

Для достижения поставленной цели в диссертационной работе необходимо решить следующие задачи:

1. Разработать метод формализованного описания процессов межсетевого взаимодействия, учитывающих особенности информационных моделей объектов доступа и характеристики современных протоколов транспортного уровня.
2. Разработать алгоритм оперативной классификации информационных виртуальных соединений на основе полиномиального представления характеристической функции, описывающей требования политики разграничения доступа на основе оценки параметров технологических виртуальных соединений.
3. Разработать алгоритм приоритетной обработки пакетного трафика, учитывающий ограничения на аппаратные ресурсы и пропускную способность сетевых каналов связи.

Объектом исследования являются классы разрешенных и запрещенных виртуальных соединений, построенных на базе современных транспортных протоколов для обмена пакетным трафиком между субъектами и объектами информационного доступа в компьютерных сетях.

Предметом исследования являются алгоритмы оперативной классификации и приоритетной обработки трафика, учитывающие ограниченность аппаратных и информационно-временных ресурсов доступных при решении задачи разграничения доступа.

Методы исследований. Для решения сформулированных задач использовался аппарат теории алгоритмов, теории защиты информации, теории

массового обслуживания и случайных процессов, методов статистической обработки данных и имитационного моделирования.

Научные результаты.

1. Представлен метод формализованного описания информационных потоков между субъектом и объектом доступа, учитывающий особенности моделей сетевых ресурсов и характеристики протоколов связи.
2. Предложен алгоритм оперативной классификации информационных виртуальных соединений при помощи полиномиального представления характеристической функции, описывающей требования политики разграничения доступа на основе оценки параметров технологических виртуальных соединений.
3. Разработан алгоритм приоритетной обработки пакетного трафика, основанный на использовании вероятностного выталкивающего механизма управления очередью ограниченного размера.

Положения, выносимые на защиту.

1. Метод формализованного описания процессов межсетевого взаимодействия, учитывающий характеристики сетевых и транспортных протоколов и особенности информационных моделей объекта доступа.
2. Алгоритм классификации информационных виртуальных соединений, позволяющий оперативно контролировать их состояние, в соответствии с требованиями политики доступа.
3. Алгоритм приоритетной обработки пакетного трафика, учитывающий ограничения на аппаратные ресурсы средств разграничения доступа и пропускную способность сетевых каналов связи.

Обоснованность и достоверность представленных в диссертационной работе научных положений подтверждается согласованностью теоретических результатов с результатами, полученными при реализации, а также апробацией основных теоретических положений в печатных трудах и докладах на всероссийских и международных научных конференциях.

Практическая ценность работы. Разработанные модели, метод и алгоритмы были использованы при создании межсетевых экранов, сертифицированных по требованиям руководящих документов ФСТЭК и ФСБ и позволяющих производить многоуровневый скрытный контроль виртуальных соединений и управление качеством доступа. В основу диссертационной работы положены результаты, полученные автором в период с 2005 по 2010 годы на кафедре «Телематика» ГОУ ВПО «СПбГПУ», а также при выполнении НИР в ГНЦ «ЦНИИ РТК».

Внедрение результатов. Результаты проведённых исследований нашли практическое применение в разработках, в которых автор принимал личное участие, в том числе:

1. При реализации алгоритмов защиты информации для управления роботом-манипулятором, находящимся на борту Международной космической станции, через сеть Интернет в рамках проведения НИОКР «Космический эксперимент Контур».
2. В рамках создания специализированной учебно-научной лаборатории и подготовке методических пособий по курсам «Методы и средства защиты компьютерной информации», «Сети ЭВМ и телекоммуникации» в ГОУ ВПО «СПбГПУ» на кафедре «Телематика».

Апробация и публикация результатов работы. Результаты, полученные в ходе работы над диссертацией, докладывались на межвузовских, всероссийских и международных научно-технических конференциях. По теме диссертации опубликовано 8 статей, в том числе – 2 в изданиях, публикации в которых рекомендуются Высшей аттестационной комиссией Министерства образования и науки Российской Федерации.

Результаты диссертационной работы получены в ходе научно-исследовательских работ, выполненных при поддержке Комитета по науке и высшей школе Правительства Санкт-Петербурга на средства грантов в сфере научной и научно-технической деятельности за 2008, 2009 и 2010 годы.

Структура и объем диссертации. Диссертационная работа общим объемом 135 страниц состоит из введения, четырех глав, заключения, списка литературы из 65 наименования, включает 29 рисунков и 1 таблицу.

СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении приводится обоснование актуальности темы диссертации, сформулированы цель и задачи исследований, перечислены основные научные результаты и положения, выносимые на защиту. Представлены сведения о внедрении результатов работы, их апробации, о публикациях, а также дана краткая характеристика содержания диссертации.

В первой главе дан анализ основных требований, принципов и технологий, которые применяются для построения и обеспечения функционирования систем защиты информации в современных КС. Приведена классификация угроз безопасности и методов РД, построенных на основе существующих субъектно-объектных моделей.

Отмечено, что для повышения эффективности решения задачи РД необходима разработка новых подходов, основанных на оперативной классификации сетевых ресурсов и рассмотрении КС как сложной виртуальной среды доступа, обладающей целым рядом специфических динамических и статистических характеристик.

Показано, что важной отличительной особенностью КС является их распределенность, требующая рассмотрения процесса РД, как сложной транзакции, построенной на основе последовательной обработки пакетного трафика ВС и учитывающей применяемую модель межсетевого взаимодействия. В этих условиях решение задачи РД должно обеспечивать заданный уровень качества функционирования информационных приложений за счет организации сетевого взаимодействия с учетом таких характеристик, как пропускная способность, задержка и вероятность потери пакетов. Это позволяет ввести новый уровень классификации информационных потоков на основе задания характеристик эффективной доступности, сформулированных в форме свойств ВС.

Таким образом, при решении задачи РД могут быть учтены требования, как к аппаратным, так и к информационным ресурсам КС, а также двойственность рассматриваемой задачи, заключающаяся в необходимости ограничения доступа, как к локальным, так и удаленным сетевым ресурсам.

Формальное описание этих особенностей может быть дано в форме моделей, при которых сетевые ресурсы и средство разграничения доступа не являются замкнутой системой, то есть изменение множества сетевых ресурсов не приводит к автоматическим изменениям компонентов средства разграничения доступа, в частности, политики безопасности.

Исходя из вышеизложенного, в данной главе обоснована необходимость разработки новых и совершенствования существующих методов и средств разграничения доступа, прежде всего межсетевых экранов (МЭ), в направлении реализации в них новых алгоритмов классификации, обеспечивающих оценку характеристик ВС в реальном масштабе времени. Так как большинство современных МЭ используются в системах РД в рамках объектно-субъектной модели описания информационного взаимодействия, то эффективным способом управления доступом к сетевым ресурсам является приоритетная обработка пакетного трафика, позволяющая учесть ограниченность аппаратных ресурсов и пропускной способности каналов связи.

На основе вышеперечисленного, в главе предложена постановка задачи исследований, которая сводится к необходимости разработки методов и алгоритмов классификации и приоритетной обработки пакетного трафика, проводимых на основе оперативной оценки состояний моделей информационных и технологических виртуальных соединений (ИВС и ТВС).

Во второй главе разработан подход к представлению требований политики РД в форме декомпозиции правил фильтрации для различных уровней описания потоков данных в форме ИВС и ТВС (рис. 1). Показано, что это позволяет существенно сократить затраты времени на решение задач классификации ВС и осуществить автоматизацию процесса настройки правил фильтрации в соответствии с требованиями политики РД и особенностями

реализации транспортных протоколов в форме одно- или двунаправленного потока пакетов, представленного моделью ТВС.

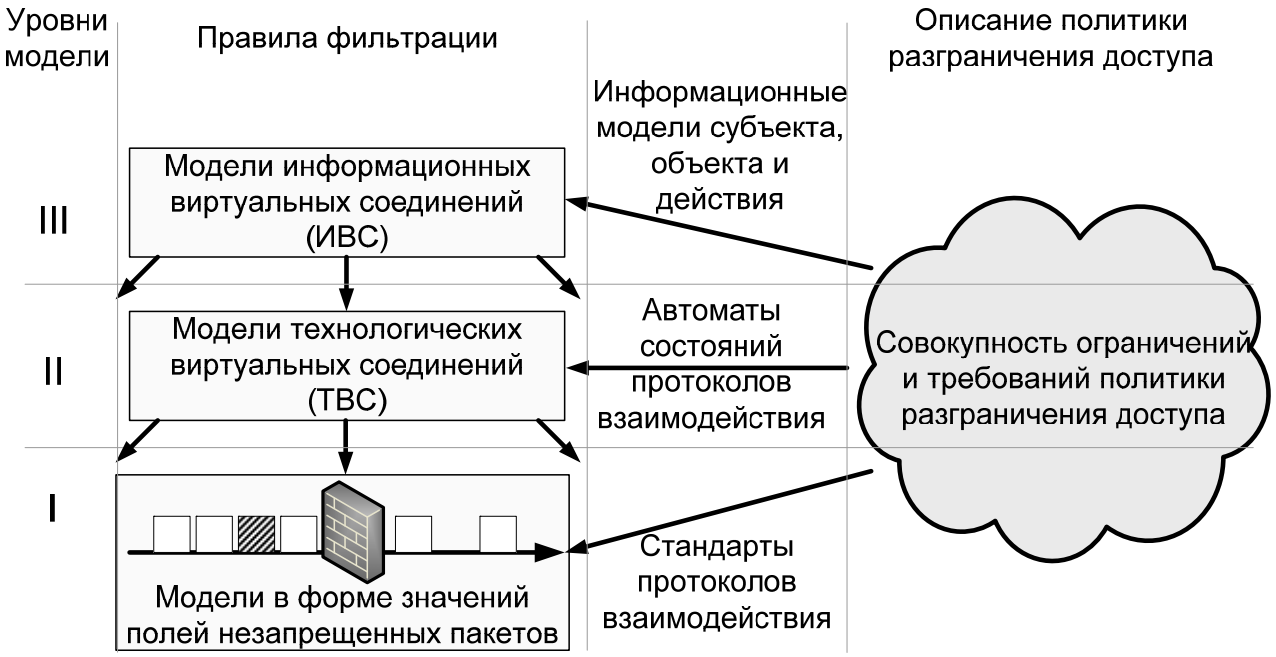

Рис. 1. Иерархическая структура формирования

требований РД при использовании моделей ИВС и ТВС

Средствами разграничения доступа модель ТВС идентифицируется как поток пакетов, формируемых сетевыми приложениями в рамках процесса информационного взаимодействия. Поэтому модель ТВС предложено представить в виде потенциально счётного подмножества декартова произведения множества пакетов P и временных меток T:

$$TBC = \{p_{t_i}\}, i = \overline{1, N}, N \in [1, \infty) \subset P \times T .$$

Такая модель ТВС характеризуется конечным набором параметров, характеризующих субъект и объект доступа, а также действие в форме потока пакетов между ними, возникающего в результате межсетевого взаимодействия. К параметрам модели относятся идентификаторы субъекта и объекта, включающие адреса, порты и прочие характеристики протоколов транспортного и сетевого уровней. Наряду с экстенсиональными параметрами, которые заданы своими значениями, в рамках предложенной модели ТВС возможно определение и других характеристик, в том числе пропускная способность, математическое ожидание и дисперсия времени передачи пакетов, корреляционная и фрактальная размерности, имеющих важное значение для решения задач РД.

Для оперативной классификации трафика, наряду с моделью ТВС, предложено использовать возможность учета характера межсетевого взаимодействия в форме модели ИВС, описывающей взаимодействие между

субъектом и объектом на уровне прикладных сервисов. Разработанная модель ИВС представляется совокупностью ТВС, число и характеристики которых определяются декартовым произведением информационных моделей взаимодействия (*ИМД*), субъекта (*ИМС*) и объекта (*ИМО*) доступа:

$$ИВС = \{ТВС_i\}, i = \overline{1, N} \subset (ИМС \times ИМД \times ИМО).$$

Разработанная формализация позволяет представить *ИМС* доступа как конечное подмножество, объем которого определяется на основе описания разрешенных субъектов межсетевого взаимодействия в рамках принятой политики РД. Поэтому *ИМС* можно характеризовать такими параметрами, как:

- идентификатор сетевого приложения;
- идентификатор пользователя или группы пользователей, инициирующих запрос сервиса;
- логические и физические адреса сетевых устройств, инициирующих формирование ИВС.

Использование модели *ИМС* позволяет рассматривать функционирование МЭ совместно с различными информационными службами КС, такими как службы каталогов в рамках протоколов Active Directory, LDAP и другие. Поэтому информация о возможностях доступа пользователей может быть представлена в форме правил фильтрации, реализуемых МЭ, при этом сами правила формируются на основе асинхронных механизмов контроля транзакции входа пользователя в сетевой домен.

Предложенная *ИМО* характеризуется конечным подмножеством информационно-сетевых ресурсов, доступ к которым разрешен в соответствии с принятой политикой РД. Параметрическая идентификация *ИМО* возможна на основе мониторинга доступных сетевых ресурсов и представляет собой оценку разрешенных характеристик, включая:

- идентификатор сетевого сервиса;
- логические и физические адреса сетевых устройств, предоставляющих информационный сервис;
- структура сетевого ресурса, участвующего в процессе информационного взаимодействия, включающая и его объектную модель, отвечающую существующим стандартам (Document Object Model).

Разработанное описание *ИМД* характеризует операции, совершаемые субъектом в рамках *ИМО*.

Показано, что разработанные модели ИВС и ТВС обеспечивают возможность оперативной классификации и приоритетной обработки пакетного трафика с учетом ограничений на процессы межсетевого взаимодействия, отвечающие политике РД. Это позволяет расширить объема понятия разрешенного ВС, включив в него приоритетные и фоновые информационные потоки, что

отвечает сетевой архитектуре типа DiffServ, в соответствии с рекомендациями RFC 2475. В результате предложено разделение ТВС на 3 класса – приоритетные, фоновые и запрещенные, что позволяет учесть требования к решению задач РД в реальном масштабе времени путем классификации потоков данных и назначении им различных приоритетов обслуживания. Так для приоритетных ТВС предоставляются сетевые ресурсы, обеспечивающие минимальное среднее значение задержек передачи пакетов или дисперсии интервалов времени между моментами потери пакетов, что непосредственно влияет на величину пропускной способности ВС. Другими словами, чем больше величина дисперсии, тем выше вероятность потерь и тем меньше пропускная способность ВС. Учитывая сложность принятия решения о классификации трафика по неполному объему передаваемых данных, в диссертации предложено ввести специальную категорию незапрещенных ВС, получивших название фоновый трафик. Общий объем введенных трех классов ТВС полностью характеризует особенности процессов информационного взаимодействия в современных КС, что позволяет, в рамках введенного формализма, доказать разрешимость задачи разграничения доступа.

В главе показано, что для совокупности приоритетных и фоновых ТВС при решении задач приоритетной обработки трафика, необходимо ввести два типа алгоритмов управления пропускной способностью, учитывающих специфику протоколов, входящих в стек TCP/IP, а именно ТВС, трафик которых обладает фрактальными свойствами (тип 1), и ТВС, трафик которых описывается с помощью марковских моделей (тип 2). Это позволяет учесть влияние ограничений пропускной способности каналов связи и аппаратных ресурсов МЭ, в частности объема сетевого буфера, на решение задачи РД. Показано, что из-за фрактального характера процессов межсетевого взаимодействия типа 1, при определении пропускной способности ТВС, необходимо учитывать не только среднее значение интервалов между потерями пакетов, но и их дисперсию, что с одной стороны усложняет алгоритмы классификации, а с другой – позволяет использовать принципы параллельной обработки данных для различных ТВС. Результаты исследований представлены на рис. 2,3,4 в форме зависимости пропускной способности ТВС ($ПС_1$ и $ПС_2$) от вероятности потери пакета (P_1 и P_2) и фрактальных свойств трафика, характеризуемых с помощью величины дисперсии (D).

В главе приведены зависимости дисперсии длины интервалов между моментами потери пакетов для введенных типов ТВС в условиях различной загруженности сети при использовании протокола TCP, в котором величина окна приемника ограничена значением в 64 сегмента, а показатель Херста H равен $H = 1 + \alpha$. Полученные аналитические зависимости представлены в форме степенной функции: $D(t) \approx (t - 64)^{1+\alpha}$, при $\alpha = 0{,}52$ для ТВС типа 1 в незагруженных сетях, $\alpha = 0{,}8$ для ТВС типа 1 в загруженных сетях и $\alpha = 0$ для

ТВС типа 2 (рис. 3). Из полученных зависимостей следует, что причиной роста дисперсии является увеличение вероятности потери пакетов, что может быть эффективно использовано для алгоритмов приоритетной обработки пакетного трафика при решении задачи РД.

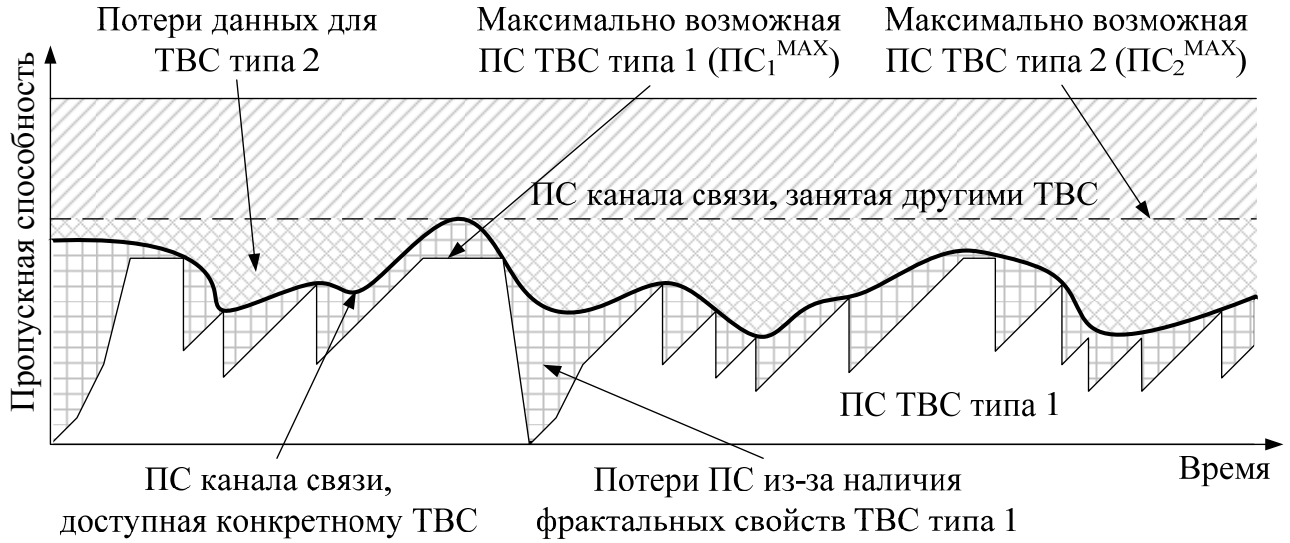

Рис. 2. Пропускная способность ТВС как основная характеристика эффективной доступности сетевых ресурсов

В главе также представлена зависимость пропускной способности ТВС от вероятности потери пакета и временных характеристик (1) виртуальных транспортных соединений (рис. 4):

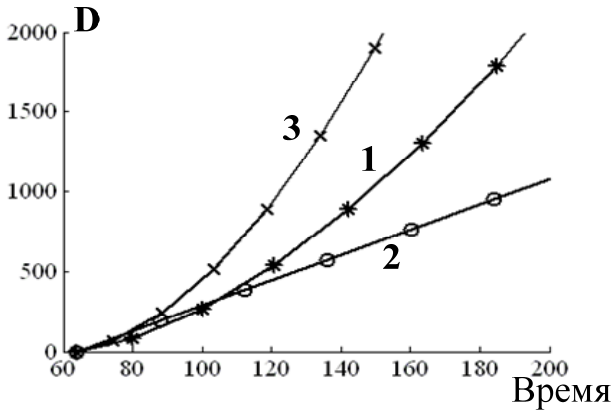

Рис. 3. Зависимость D от времени существования ТВС для α=0,52 – «1», α=0,8 – «2» и α=0 – «3»

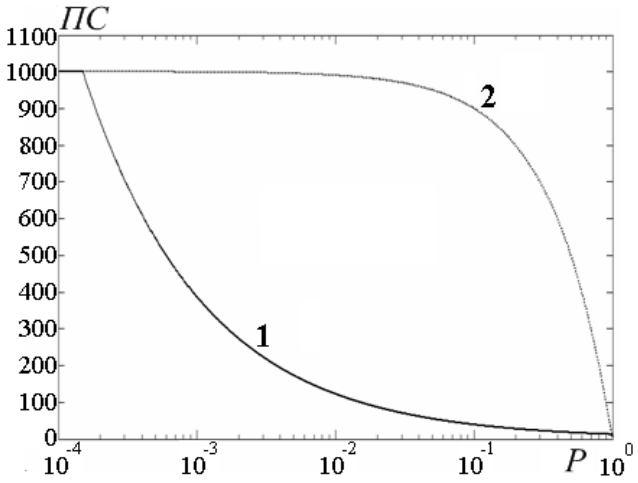

Рис. 4. Зависимость $ПС_1(P_1)$ – «1» и $ПС_2(P_2)$ – «2»

$$ПС_1(P_1) = \min(ПС_1^{MAX}; 1/\ RTT \cdot \sqrt{\frac{2}{3}P_1}), \quad ПС_2(P_2) = ПС_2^{MAX}(1-P_2), \qquad (1)$$

в формуле (1) параметр RTT характеризует время между отправкой пакета и получением подтверждения о доставке для протокола TCP. Полученные

зависимости используются для построения алгоритмов приоритетной обработки трафика ТВС типа 1 и 2 при решении задач РД.

На основании описанных выше результатов, в главе предложен алгоритм оперативной классификации, позволяющий ввести адаптивно конфигурируемый набор правил фильтрации трафика (контролирующих правил) для каждого типа ТВС. Разработанный алгоритм формирования контролирующих правил позволяет для каждого из сетевых пакетов представить законченную последовательность операций, гарантированно приводящую к принятию решения в рамках введенных трех классов ТВС (рис. 5). Процесс разделения трафика формируется как иерархическая последовательность операций, начинающаяся с правила $\alpha_0 = (\alpha_{01}, \alpha_{02}, ..., \alpha_{0N})$, которое применяет набор классифицирующих предикатных отношений ко всей наблюдаемой совокупности пакетов. Особенностью реализации задачи РД в КС является то, что окончательная классификации ТВС возможна только после его завершения, поэтому при решении задачи РД приходится вычислять характеристическую функцию ТВС по неполным данным.

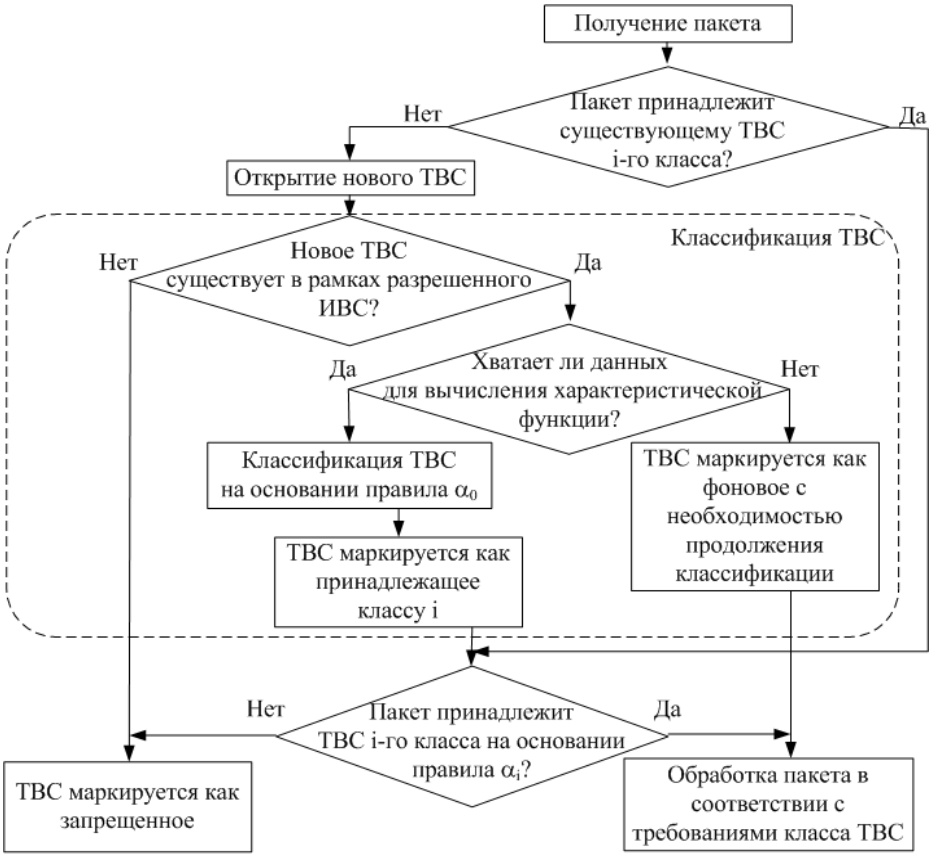

Рис. 5. Алгоритм классификации ТВС

Предложенный алгоритм учитывает тот факт, что если в поступивших пакетах не содержится данных необходимых для вычисления характеристической функции для правила α_0, то инициируемое ими ТВС маркируется как фоновое, а решение по РД является отложенным, и для завершения вычисления характеристической функции ожидаются следующие пакеты. Таким образом, для каждого ТВС в соответствии моделью ИВС характеристическая функция вычисляется в форме полинома Жегалкина, количество членов которого может быть изменено для повышения точности классификации. Очевидно, что если данных для принятия

решения достаточно, то по результатам работы правила α_0 вновь организованное соединение относится к одному из M вариантов представления требований политики РД для различных классов ТВС. Это позволяет повысить производительность средств разграничения доступа, так как каждый класс ТВС контролируется определенным набором правил ($\alpha_1 = (\alpha_{11}, \alpha_{12}, ..., \alpha_{1H})$, $\alpha_2 = (\alpha_{21}, \alpha_{22}, ..., \alpha_{2J})$, … , $\alpha_M = (\alpha_{M1}, \alpha_{M2}, ..., \alpha_{ML})$). Так как правила $\{\alpha_{ij}\}, i = \overline{0, M}, j \in N$ представляются в аддитивной форме предикатного полинома, это позволяет адаптировать свойства характеристической функции к требованиям политики РД путем ее реконфигурации при добавлении новых ограничений. Если совокупность пакетов перестает удовлетворять контролирующим правилам своего класса, то все пакеты данного ТВС маркируются как запрещенные, что позволяет оперативно контролировать текущее состояние ТВС, в соответствии с требованиями политики доступа.

В третьей главе проведена математическая формализация алгоритма приоритетной обработки пакетного трафика для решения задачи разграничения доступа с учетом предложенных моделей. Поскольку основным фактором, осложняющим использование моделей сетевого трафика в реальном масштабе времени, служит громоздкость численного решения задач теории массового обслуживания, в главе предлагается использовать аналитический подход, основанный на использовании вероятностного выталкивающего механизма управления очередью ограниченного размера. Разработанный подход основан на существенном использовании особенностей межсетевого взаимодействия, возникающих в загруженных сетях при прохождении через них различных классов сетевого трафика в соответствии с моделью типа $\vec{M}_2 / M / 1 / k / f_2^1$.

В данной модели приоритетный и неприоритетный входящие потоки пакетов образуются совокупностью незапрещенных ТВС типа 1 и 2. В этом случае применение марковской модели может быть обосновано предельной теоремой для случайных потоков, представляющих собой суперпозицию большого числа элементарных потоков, ни один из которых не является доминирующим в сумме, поэтому результирующий поток можно считать близким к простейшему.

Обработка пакетов с использованием экспоненциального распределение времени обслуживания может быть обоснована теоремой инвариантности, в соответствии с которой результаты, полученные для простейших потоков, могут быть корректно применены к случаю общих распределений, если для интенсивности процесса обслуживания взята величина, равная $\mu = \frac{1}{\bar{x}} = 1 \Big/ \int_0^\infty x \cdot b(x) dx$, где $b(x)$ – функция распределения реального времени обслуживания.

В результате для СМО типа $\vec{M}_2/M/1/k/f_2^1$ может быть представлен размеченный граф состояний, на основе которого составляется система линейных уравнений (2). Сложность численного решения этих уравнений пропорциональна величине $k(k-1)/2$, в которой k характеризует ограничение на размер буферной памяти, используемой в процессе обработки пакетов. В главе показано, что решение данной системы стандартными методами требует больших вычислительных ресурсов и невозможно в реальном масштабе времени.

Поэтому для решения сформулированной задачи предложено преобразование уравнений состояния (2) методом производящих функций Вайта-Кристи-Стефана (3), позволяющим сократить сложность численного решения представленной задачи до значения равного $k+1$. Полученное решение представлено формулой (4), в котором числовые коэффициенты ζ_i и $\xi_{i,j}$ выражаются через полиномы Гегенбауэра (5).

$$\begin{aligned}&-[\lambda_1(1-\delta_{j,k-i})+\alpha\lambda_1(1-\delta_{j,k})\delta_{j,k-i}+\lambda_2(1-\delta_{j,k-i})+\mu(1-\delta_{i,0}\delta_{j,0})]p_{ij}+\mu p_{i+1,j}+\\&+\mu\delta_{i,0}p_{i,j+1}+\lambda_2 p_{i,j-1}+\lambda_1 p_{i-1,j}+\alpha\lambda_1\delta_{j,k-i}p_{i-1,j+1}=0,\qquad (i=\overline{0,k};\ j=\overline{0,k-i}),\end{aligned} \tag{2}$$

$$G(u,v)=\sum_{i=0}^{k}\sum_{j=0}^{k-i}p_{ij}u^i v^j \tag{3}$$

$$\begin{aligned}p_i&=\frac{\rho_1^{-1}(\rho_1^{-i}-\zeta_{i+1})p_0+\sum_{j=1}^{i-1}[(1-\alpha)\rho_1^{j-i-1}-\xi_{i+1,j}]p_j}{\xi_{i+1,i}-(1-\alpha)\rho_1^{-1}},\qquad (i=\overline{1,k-1})\\ p_k&=\frac{\rho_2(1-r_k)-\alpha\rho_1(r_k-p_0)+r_0-\rho_1^{-1}\zeta_k p_0-\sum_{j=1}^{k-1}\xi_{k,j}p_j}{(1-\alpha)},\end{aligned} \tag{4}$$

$$\zeta_i=\sum_{j=0}^{i-1}[C_{i-j-1}^{j+1}(t_0)-C_{i-j-2}^{j+1}(t_0)]\beta^j,(i=\overline{1,k})$$

$$\xi_{i,j}=\sum_{s=j}^{i}\{\rho_1^{-1}[C_{i-s-1}^{s-j+1}(t_0)-C_{i-s-2}^{s-j+1}(t_0)]-\alpha[C_{i-s}^{s-j+1}(t_0)-C_{i-s-1}^{s-j+1}(t_0)]\}\beta^{s-j}, \tag{5}$$

$$(i=\overline{2,k};\ j=\overline{0,i-1})$$

где λ_i – интенсивность i-го входящего потока ($i=1$ – это поток пакетов приоритетных ТВС, $i=2$ – фоновых), $\delta_{i,j}$ – дельта-символ Кронекера, p_{ij} – вероятность нахождения в системе i-го числа приоритетных пакетов и j-го – фоновых, $\rho_i=\lambda_i/\mu$ – коэффициент загруженности системы по i-му типу

требований, $p_i = p_{k-i,i}$ при $(i = \overline{0,k})$, $\beta = -\rho_2 \rho_1^{-1/2}$, $t_0 = t(0) = 1/2(1+\rho_1+\rho_2)\rho_1^{-1/2}$ – коэффициенты полиномов Гегенбауэра, α – управляющий параметр, характеризующий вероятность выталкивания неприоритетных пакетов из буферной памяти в устройстве приоритетной обработки пакетного трафика.

Использование уравнений (4) и (5) вместо (2) позволяет существенно сократить время вычисления управляющего параметра α, и на этом основании решать задачу приоритетной обработки незапрещенного трафика в реальном масштабе времени в различных режимах функционирования КС, в том числе в режимах перегрузки.

Проведено сравнение абсолютного и относительного механизмов обслуживания, а также исследование свойств сетевых процессов при различном уровне загруженности сети. Показано, что для задачи разграничения доступа использование абсолютного приоритета предпочтительнее. Рассмотрены ограничения на загруженность канала связи, в рамках которых целесообразно использовать предлагаемое решение $(1 \le \rho_1 + \rho_2 < 2{,}5)$. Показано, что в слабозагруженных сетях при значениях $\rho_1 + \rho_2 < 1$ и в сильнозагруженных при $\rho_1 + \rho_2 > 2{,}5$ вероятность потери пакетов может быть получена путем линейной аппроксимации аналитических решений систем типа $\vec{M}_2 / M / 1 / k / f_2^0$ и $\vec{M}_2 / M / 1 / k / f_2^2$.

В четвертой главе рассмотрены вопросы реализации и практического внедрения полученных результатов. Дано описание функционирования средств разграничения доступа, реализующего предложенные алгоритмы классификации и приоритетной обработки пакетного трафика. В главе представлены оценки, характеризующие эффективность разработанных моделей и алгоритмов разграничения доступа, включая управление пропускной способностью виртуальных транспортных соединений. Оценки получены в рамках международного космического эксперимента «Контур» при управлении удаленным робототехническим объектом на борту Международной космической станции с использованием КС для передачи мультимедийного трафика через сегменты сети Интернет и каналы спутниковой связи.

Представлены оценки влияния ширины доступной полосы пропускания на эффективности решения задачи РД в условиях влияния помех и других неблагоприятных факторов, характерных для использования беспроводных, в том числе спутниковых каналов связи. Полученные результаты подтверждают возможность повышения точности классификации трафика на основе использования разработанного алгоритма декомпозиции потоков пакетов на ИВС и ТВС. Показано, что предложенные методы упрощения аналитического описания задач СМО при приоритетной обработке трафика позволяют решать задачи РД в реально масштабе времени и стабилизировать пропускную способность, а также уменьшить дисперсию задержки приоритетных ТВС.

Реализованные модели и алгоритмы вошли в состав программного обеспечения МЭ ССПТ-2, сертифицированного по требованиям ФСТЭК и ФСБ для применения в современных высокоскоростных КС, построенных на базе технологии Ethernet с пропускной способностью 10/100/1000 Мбит/с, и поддерживает одновременную обработку до 40000 ТВС.

Важной особенностью разработанных алгоритмов является возможность их применения в МЭ, функционирующим в режиме скрытной фильтрации, что повышает его защищенность и общую надежность системы РД, созданной на его основе.

Основные результаты работы

1. Предложен метод формализованного описания процессов межсетевого взаимодействия, учитывающих особенности информационных моделей объектов доступа и характеристики современных протоколов.
2. Разработан алгоритм оперативной классификации информационных виртуальных соединений на основе полиномиального представления характеристической функции, описывающей требования политики разграничения доступа на основе оценки параметров технологических виртуальных соединений и повышающий производительность средств разграничения доступа.
3. Разработан алгоритм приоритетной обработки пакетного трафика, позволяющий решать задачу приоритетной обработки пакетного трафика в реальном масштабе времени в различных режимах функционирования компьютерной сети, в том числе в режимах перегрузки.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. **Городецкий, А.Я. Пропускная способность компьютерных сетей с фрактальными свойствами / А.Я. Городецкий, В.С. Заборовский, В.А. Мулюха // Научно-технические ведомости СПбГПУ. – 2009. – №3. – С. 12-18.**
2. **Городецкий, А.Я. Экспериментальное исследование статистических свойств сетевой среды на основе анализа ансамбля TCP-соединений / А.Я. Городецкий, В.С. Заборовский, И.А. Завалей, В.А. Мулюха // Научно-технические ведомости СПбГПУ. – 2008. – №2. – С. 26-31.**
3. Vladimir .Zaborovsky Transport Layer Management and Security in Highly Loaded Computer Networks / Vladimir .Zaborovsky, Oleg Zayats, Vladimir Mulukha, Sergey Kupreenko // Worldcomp'10, Proceedings of The 2010 International Conference on Security and Management, Volume II, Las Vegas, Nevada, USA, 2010. – Published by CSREA Press. – USA 2010. – p.30-35.

4. Zaborovsky Vladimir Active Queuing Management for Telematics Space Network Robotics System \ Управление телематическими робототехническими системами космического назначения на основе приоритетной обработки сетевого трафика. ЭКСТРЕМАЛЬНАЯ РОБОТОТЕХНИКА / Zaborovsky Vladimir, Zayats Oleg, Mulukha Vladimir // Труды XXI Международной научно-технической конференции. – Санкт-Петербург: Изд-во «Политехника-сервис», 2010. – С. 340-349.

5. Vladimir Zaborovsky Priority Queueing With Finite Buffer Size and Randomized Push-out Mechanism / Vladimir Zaborovsky, Oleg Zayats, Vladimir Mulukha // Proceedings of The Ninth International Conference on Networks (ICN 2010), Menuires, The Three Valleys, French Alps, 11-16 April 2010. – Published by IEEE Computer Society. – 2010. – p.316-320

6. Vladimir Zaborovsky Internet Performance: TCP in Stochastic Network Environment / Vladimir Zaborovsky, Aleksander Gorodetsky, Vladimir Muljukha // Proceedings of The First International Conference on Evolving Internet INTERNET 2009, 23-29 August 2009, Cannes/La Bocca, France. – Published by IEEE Computer Society. – 2009. – p.447-452

7. Заборовский В.С. Исследование статистических свойств сетевой среды на основе анализа ансамбля TCP-соединений / В.С. Заборовский, В.А. Мулюха // XXXVII неделя науки СПбГПУ, Материалы Всероссийской межвузовской научно-технической конференции студентов и аспирантов, 24 - 29 ноября 2008 года, Часть XVII, факультет при ЦНИИ робототехники и технической кибернетики. – СПб.: Изд-во Политехнического университета. – 2008. – С. 23-24

8. Заборовский, В.С. Статистические модели сетевой среды в условиях устойчивого неравновесия / В.С. Заборовский, И.А. Завалей, В.А. Мулюха // Материалы XII Всероссийской конференции по проблемам науки и высшей школы. – СПб.: Изд-во Политехнического университета. – 2008. – С. 28-34