На правах рукописи

ЛУКАШИН Алексей Андреевич

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

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

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2012

Работа выполнена в федеральном государственном бюджетном 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,
профессор Санкт-Петербургского государственного политехнического университета
Зегжда Дмитрий Петрович

кандидат технических наук,
начальник отдела
ООО «Технологии автоматизации и программирования»
Старовойтов Михаил Александрович

Ведущая организация: ФГУП НИИ «КВАНТ», г. Москва

Защита состоится « » декабря 2012 г. в часов на заседании диссертационного совета Д 212.229.27 при ФГБОУ 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 ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет»

Автореферат разослан « » ноября 2012г.

Ученый секретарь
диссертационного совета:
Платонов Владимир Владимирович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертации

Развитие сетевых технологий в направлении создания сред облачных вычислений (СОВ) предъявляет новые требования к средствам разграничения доступа (РД) к информационным сервисам – одному из основных компонент современных систем информационной безопасности (ИБ). Эти требования вытекают из необходимости учета динамического характера процессов выделения вычислительных и сетевых ресурсов при конфигурации виртуальных машин (ВМ) и структуры адресного пространства, используемого для доступа к информационным сервисам. Описание политики доступа (ПД) может быть представлено с помощью правил фильтрации (ПФ) сетевого трафика, структура и параметры которых генерируются в процессе функционирования СОВ и сервисов, реализуемых с использованием ВМ. При этом необходимо учитывать требования сохранения целостности ПД, аналогично тому, как в условиях изменения сетевой топологии для сохранения информационной связанности ресурсов в Интернет используются протоколы динамической маршрутизации. Поэтому при использовании СОВ для размещения информационных сервисов особую актуальность приобретает сложная научно-техническая задача развития технологии защиты информации, обеспечивающей выполнение требований ПД в сетевой среде с динамически изменяющимися характеристиками.

Важность этой задачи отмечается как российскими, так и зарубежными учёными, в том числе Н.А. Гайдамакиным, П.Д. Зегждой, В.Ю. Скибой, М. Сриватса, Т. Вангом и др.

Перспективным направлением решения задачи РД в СОВ является использование технологии межсетевого экранирования с учетом динамики структуры и параметров защищаемой сетевой среды. Применение этой технологии основано на модели РД к информационным сервисам в СОВ, отражающей требования ПД. Такая модель может быть представлена с использованием динамически формируемого набора правил фильтрации, в соответствии с состоянием информационных сервисов. Однако возрастающая сложность алгоритмов фильтрации предъявляет высокие требования к производительности межсетевых экранов (МСЭ), что делает необходимым использование методов параллельной обработки информационных потоков с помощью ВМ, реализующих сервис РД на базе многоядерных микропроцессоров. Предложенное направление развития сервиса РД требует разработки метода динамического формирования ПФ для межсетевых экранов (МСЭ), разработки взаимно согласованного набора алгоритмов фильтрации сетевых соединений, не соответствующих требованиям ПД, и создания архитектуры программного обеспечения для виртуальных машин,

выполняющих функции МСЭ, реализующих политику доступа в СОВ. В современной литературе подход к созданию сложных технических систем, связанность которых обеспечивается за счет организации процессов обмена информацией по сети, получил название сетецентрического. Этот подход применительно к задаче РД требует обеспечения ситуационной осведомленности и локальности действий каждого из межсетевых экранов, входящих в группировку ВМ, используемых в СОВ для реализации ПД.

Целью исследования является разработка метода и алгоритмов защиты информационного взаимодействия с использованием межсетевых экранов в среде облачных вычислений.

Для достижения поставленной цели в диссертационной работе решены следующие задачи.

1. Разработана модель информационного взаимодействия для описания процессов разграничения доступа к информационным сервисам, учитывающая динамические характеристики среды облачных вычислений.
2. Разработан метод конфигурации межсетевых экранов, основанный на динамическом формировании правил фильтрации в соответствии с изменяющимися параметрами информационного взаимодействия.
3. Разработан параллельный алгоритм фильтрации виртуальных соединений, позволяющий повысить производительность работы межсетевых экранов.
4. Разработана архитектура системы защиты информационного взаимодействия, обеспечивающей выполнение заданной политики доступа.

Методы исследования: для решения сформулированных задач использовался аппарат теории алгоритмов, теории защиты информации, системного анализа и теории категорий.

Объект исследования: система разграничения доступа к информационным сервисам в среде облачных вычислений.

Предмет исследования: методы и алгоритмы динамической конфигурации межсетевых экранов в среде облачных вычислений, реализующие сетецентрический подход к организации системы разграничения доступа.

Научная новизна работы результатов диссертации заключается в следующих аспектах.

1. В разработке модели состояния сетевой среды в задачах разграничения доступа с использованием теории категорий.
2. В создании метода динамического формирования правил фильтрации для межсетевых экранов в условиях изменяющейся структуры связей между субъектами и объектами информационного взаимодействия.
3. В разработке архитектуры системы защиты информационного взаимодействия, обеспечивающей выполнение заданной политики доступа.

Положения, выносимые на защиту

1. Модель информационного взаимодействия для описания процессов разграничения доступа к информационным сервисам, учитывающая динамические характеристики среды облачных вычислений.
2. Метод конфигурации межсетевых экранов, основанный на динамическом формировании правил фильтрации в соответствии с изменяющимися параметрами информационного взаимодействия.
3. Параллельный алгоритм фильтрации виртуальных соединений, позволяющий повысить производительность работы межсетевых экранов.
4. Архитектура системы защиты информационного взаимодействия, обеспечивающая выполнение заданной политики доступа.

Обоснованность и достоверность представленных в диссертационной работе научных положений обеспечивается проведением анализа исследований в данной области и апробацией полученных результатов в печатных трудах и докладах на всероссийских и международных научных конференциях.

Практическая значимость работы. Разработанные модели, методы и алгоритмы могут быть использованы для решения задач РД в СОВ и виртуализованных центрах обработки данных. Внедрение созданных средств РД позволяет осуществить контроль сетевого трафика, передаваемого по нефизическим каналам связи, обеспечиваемых гипервизорами СОВ. Разработанные методы и алгоритмы параллельной обработки сетевого трафика обеспечат развитие технологии межсетевого экранирования и повышение функциональных возможностей систем РД. Результаты, полученные в диссертационной работе, использованы при создании межсетевых экранов, сертифицированных по требованиям руководящих документов ФСТЭК и ФСБ, позволяющих осуществлять РД в скрытном режиме. Также результаты исследований использованы в научно-исследовательском проекте разработки защищенной среды облачных вычислений «Пилигрим», выполняемом в ГНЦ «ЦНИИ РТК» и при выполнении НИР на кафедре телематики ФГБОУ ВПО «СПбГПУ».

Апробация и публикация результатов работы. Основные положения и результаты диссертационной работы докладывались на межвузовских, всероссийских и международных научных конференциях, среди которых: СКТ 2010 (Россия, Дивноморск, 2010), ПАВТ 2011 (Россия, Москва 2011), IEEESMC 2011 (США, Аляска, 2011), INTERNET 2012 (Италия, Венеция, 2012), а также на промышленной выставке «Связь-Экспокомм 2012». По теме диссертации опубликовано 11 работ, в том числе 4 статьи в изданиях, входящих в перечень Высшей аттестационной комиссии 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 гранта в сфере научной и научно-технической деятельности за 2012 год.

Структура и объем диссертационной работы. Диссертационная работа объемом 140 машинописных страниц, содержит введение, четыре главы и заключение, список литературы, содержащий 91 наименование, 15 таблиц и 34 рисунка.

СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснована важность и актуальность темы диссертации, определены цель и задачи исследований, показана научная новизна и практическая значимость.

В первой главе диссертации приведена общая характеристика современных моделей, методов и механизмов решения задачи РД в компьютерных сетях. Представлены субъектно-объектная модель РД и понятие монитора безопасности. В качестве средства РД рассмотрен межсетевой экран, выполняющий роль монитора безопасности в компьютерных сетях. Приведены особенности СОВ: виртуализация вычислительных ресурсов, осуществление информационного обмена между ВМ по программно-эмулируемым каналам связи и наличие сервисов управления СОВ. Введены понятия информационного сервиса (ИС) СОВ – программного компонента, функционирующего в ВМ СОВ, и понятие управляющего сервиса (УС) СОВ – программного компонента, осуществляющего управление гипервизорами, пользователями и ВМ в СОВ. Доступ к ИС и УС осуществляется по сети. 1. В качестве модели угроз рассматриваются угрозы нарушения политики безопасности при доступе к ИС или к УС СОВ. Модель нарушителя, рассматриваемая в работе, включает два основных типа нарушителей: внешний нарушитель, не имеющий прав доступа к СОВ, осуществляющий попытку доступа к ИС или УС, и внутренний пользователь, осуществляющий попытку запрещенного доступа к ИС других пользователей или к УС СОВ. МСЭ

осуществляет разграничение доступа к ИС и УС с помощью ПФ, содержащих параметры адресов канального и сетевого уровней, портов транспортного уровня и используемых прикладных протоколов стека TCP/IP. Спецификой СОВ является динамическое перераспределение сетевых (IP) адресов между ВМ и динамическое изменение множества ВМ в СОВ.

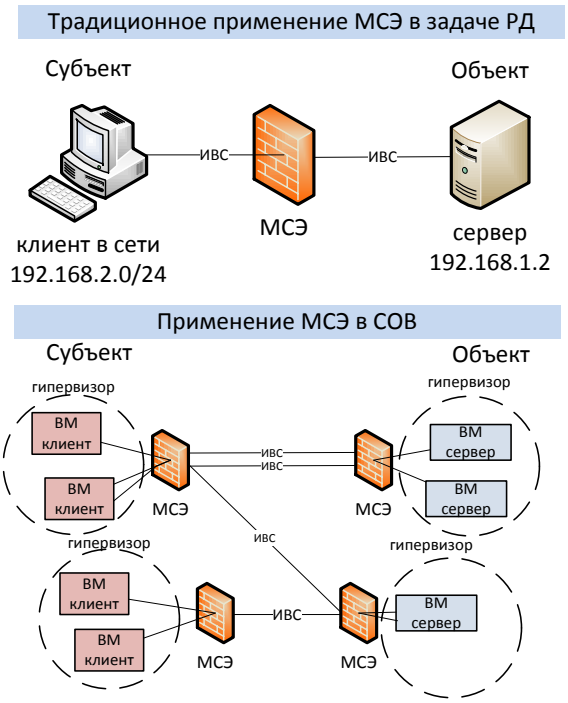

Рисунок 1. Специфика применения МСЭ в СОВ

Для учета специфики СОВ необходимо перейти от статического задания ПФ в МСЭ к динамически формируемому множеству ПФ в соответствии с текущей сетевой конфигурацией функционирующих в СОВ ВМ и осуществлять фильтрацию информационного взаимодействия между ВМ, принадлежащим разным пользователям СОВ. Для этого необходимо наличие МСЭ в каждом гипервизоре СОВ (рисунок 1). Система РД становится распределенной и МСЭ должны согласовано обеспечивать выполнение ПД, поэтому необходима разработка новых подходов к организации системы защиты, которые основываются на информационной связанности её компонент. Рассмотрен сетецентрический принцип организации систем, который основывается на целостности, информационной связанности и локальности принятия решений. Применительно к задаче РД в СОВ сетецентричность расширяет возможности поддержания в актуальном состоянии описания информационно-вычислительных ресурсов, необходимого для решения задачи РД в СОВ. Отмечено, что новые методы и алгоритмы РД в СОВ предъявляют повышенные требования к вычислительным возможностям средств разграничения доступа. Поэтому необходима разработка новых подходов к организации контроля информационного взаимодействия, которые базируются на использовании параллельных алгоритмов и многоядерной архитектуре аппаратной платформы компонент СОВ. Предложен метод интеграции МСЭ в СОВ в виде ВМ, которые используют вычислительные ресурсы СОВ. Такой подход позволяет осуществить фильтрацию трафика между ВМ, функционирующими в одном гипервизоре, и снизить затраты на систему защиты, избежав необходимости подключения дополнительного аппаратного обеспечения.

На основе вышеперечисленного, в главе сформулирована постановка задачи исследования, которая сводится к разработке методов и алгоритмов РД к информационным сервисам с использованием межсетевых экранов в среде облачных вычислений.

Во второй главе рассмотрена модель информационного взаимодействия в форме «субъект-действие-объект». Субъектом взаимодействия S является активная сущность компьютерной сети. Объектом O является пассивная сущность в компьютерной сети, предоставляющая запрашиваемый сервис прикладного уровня. Действие характеризует информационный обмен между субъектом и объектом, который длится во времени, является двунаправленным обменом пакетами в компьютерной сети и описывается в форме информационного виртуального соединения (ИВС). РД к информационным сервисам – это возможность блокировки (фильтрации) или разрешения ИВС в соответствии с требованиями ПД. Формально информационное взаимодействие в СОВ можно представить в виде множества ИВС $\text{ИВС} = \text{ИВС}_\text{р} \cup \text{ИВС}_\text{з}$, где $\text{ИВС}_\text{р}$ – множество разрешенных ПД потоков, $\text{ИВС}_\text{з}$ – множество запрещенных ПД потоков, причем $\text{ИВС}_\text{р} \cap \text{ИВС}_\text{з} = \emptyset$. Задача РД доступа сводится к фильтрации потоков $\text{ИВС}_\text{з}$. «Доступ» трактуется, как возможность передачи пакетов от субъекта к объекту. ИВС реализуется в виде множества технологических виртуальных соединений (ТВС), которые в компьютерной сети представлены сетевыми соединениями между субъектом и объектом взаимодействия по протоколам транспортного уровня, такими как TCP или UDP. Модель ТВС представлена в виде потенциально счетного подмножества декартова произведения пакетов P и временных меток T:

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

Модель ИВС представлена в виде совокупности ТВС:

$$IVC = \{TVC_i\}, i = \overline{1..N}$$

Задача МСЭ, как средства РД в компьютерной сети СОВ, сводится к фильтрации ТВС и принятии решения о запрете или разрешении ИВС на основе имеющихся у МСЭ ПФ, поэтому для решения задачи РД в СОВ необходимо обеспечить конфигурацию МСЭ правилами фильтрации, обеспечивающими выполнение ПД в текущих условиях. Для описания процессов преобразования ПД в правила фильтрации (ПФ) для МСЭ согласно текущему состоянию СОВ использован формализм теории категорий, которая изучает свойства совокупности отображений, абстрагируясь от структуры описываемых объектов. Категория является конструкцией, позволяющей описать системы (объекты) и процессы переходов между ними (морфизмы). Для контроля информационного взаимодействия в СОВ система РД должна

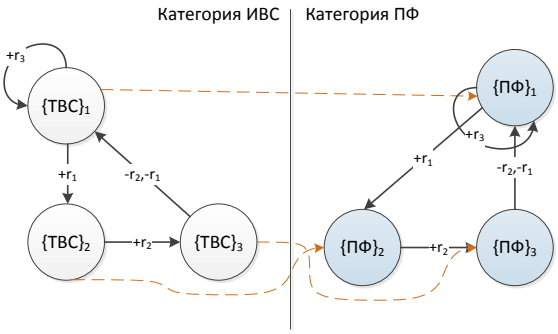

Рисунок 2. Категории ИВС и ПФ

выполнять преобразования вида ПД → ПФ при каждом изменении состояния среды. На этапе формирования ПД неизвестен состав информационных сервисов СОВ, которые могут появляться и исчезать в процессе функционирования СОВ. Физические и логические адреса ВМ могут измениться, что делает необходимым динамическое изменение ПФ для МСЭ.

Для формализации вышеописанных процессов введена категория ИВС. Объектом данной категории является подмножество ТВС $o = \{tvc_i\}, i = \overline{1..n}$, которые формируют ИВС, а морфизмами категории ИВС являются операции запуска и остановки ВМ в СОВ. Для структурированного представления ПД в форме ПФ для ИВС введена категория ПФ, объектами которой являются подмножества правил фильтрации $rules = \{rules_i\}, i = \overline{1..n}$, а морфизмами операции изменения множества ПФ, необходимого для выполнения ПД.

Для описания процесса перехода от ИВС к правилам фильтрации введен функтор T: ИВС → ПФ, переводящий объекты категории ИВС в объекты категории ПФ, необходимые для контроля ИВС, с сохранением морфизмов между объектами (рисунок 2).

Для классификации ИВС на соответствие ПД в СОВ использована ролевая (RBAC) модель РД, которая формально может быть представлена в виде совокупности следующих параметров:

$$\theta =< U, \Re, P, C >,$$

$U = \{u_i\}, i = \overline{1..n}$ – множество идентификаторов пользователей СОВ, которые осуществляют управление ВМ и информационными сервисами. Р – множество привилегий в форме описания разрешенных информационных сервисов, задаваемых в следующим образом:

- пользователь СОВ $u \in U$, предоставляющий информационный сервис;
- $rul = \{r_i\}, i = \overline{1..N}$ – множество правил, идентифицирующих ИС. Правило $r =< transport, port, protocol, ext >$, где transport – транспортный протокол, порт – порт по которому функционирует ИС, protocol – прикладной протокол, ext – дополнительные признаки для полей заданного прикладного протокола.

Например, привилегия может быть задана следующим образом: {user:Ivan, [{transport:”TCP”, port:”80”, protocol:”HTTP”, ext:[{method:”GET”}]}]}. Данная привилегия задает правило доступа к веб серверу по протоколу http с использованием метода GET по 80 порту к ВМ, принадлежащим пользователю Ivan.

$\Re$ - множество ролей, которые могут быть назначены пользователям. Роль задана в виде множества привилегий $r = \{p_i\}, i = \overline{1..n}, r \subset P$. С – множество сеансов пользователей в СОВ, элементами которого являются объекты категории ИВС.

Модель информационного взаимодействия в СОВ с точки зрения задачи РД к ИС в терминах процессов межсетевого взаимодействия ζ может быть представлена в виде совокупности следующих составляющих:

$$\zeta =< N_{vm}, N_{man}, Rul_{vm}, Rul_{man}, VM, V, \theta >$$

Информационное взаимодействие в СОВ разделено на две части, которые представлены подсетью управления N_{man}, и подсетью виртуальных машин N_{vm}. Каждая подсеть задана множеством IP адресов, которые могут быть назначены виртуальным машинам или серверам, обеспечивающим функционирование СОВ соответственно. Политика доступа к управляющим сервисам СОВ, функционирующим в подсети N_{man}, задана в виде набора ПФ $Rul_{man} = \{rul_{man_i}\}, i = \overline{1..n}$. VM – множество ВМ, функционирующих в СОВ. Элементами множества $VM \subset N_{vm}$ являются IP адреса ВМ, которые функционируют в СОВ. Текущие сетевые соединения, установленные в СОВ, представлены множеством ТВС $V = \{TVC_i\}, i = \overline{1..n}$. Информационный обмен в СОВ представлен в виде ТВС в подсети управления V_{man} и ТВС между ВМ V_{vm} со следующими ограничениями:

$$V_{VM} = \{v_i\}, i \in \overline{1..k}, V_{VM} \subset V, V_{man} = \{v_i\}, i = \overline{1..k}, V_{man} \subset V, V = V_{vm} \cup V_{man}$$

$$\forall v \in V_{vm}: A_s \in VM, A_o \in VM, \qquad \forall v \in V_{vm}: r_o \in VM, r_s \in VM, u_o \in U, u_s \in U,$$
$$\forall v \in V_{man}: A_s \in N_{man}, A_o \in N_{man},$$

где A_s – сетевой адрес субъекта информационного взаимодействия, A_o – сетевой адрес объекта информационного взаимодействия. r_o – ВМ, в которой функционирует ИС (объект), u_o – пользователь СОВ, представляющий ИС. r_s – ВМ, в которой функционирует приложение осуществляющее доступ к ИС (субъект), u_s – пользователь СОВ, осуществляющий доступ к ИС. Субъект и объект информационного взаимодействия, осуществляющие обмен данными с помощью ТВС, действуют с привилегиями пользователей СОВ, которые осуществили запуск виртуальных машин, между которыми осуществляется взаимодействие.

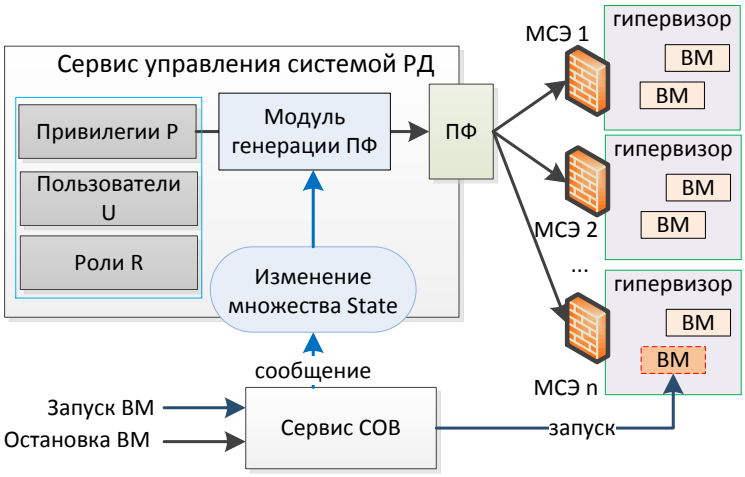

Рисунок 3. Генерация ПФ для МСЭ

Состояние СОВ задано множеством IP адресов ВМ с метками пользователей:

$$State = \{vm_{u_i}\}, i = \overline{1..n},\ State \subset VM \times U.$$

При изменении множества $State$ необходимо осуществить генерацию ПФ Rul_{vm} и загрузить новый набор правил в МСЭ. Для этого разработан метод динамической конфигурации ПФ для межсетевых экранов в системе РД в СОВ. При получении команды об остановке или запуске ВМ сервис управления системой РД осуществляет генерацию ПФ и их распределение по МСЭ (рисунок 3).

Операция генерации ПФ для привилегии p, реализуется путем подстановки IP адресов субъекта a_s (адреса ВМ пользователя, обладающего привилегией) и объекта a_o (адреса ВМ пользователя, предоставляющего ИС) в каждое правило rul привилегии $p \in P$ обозначена $gen(a_s, a_o, p)$:

$$(p =< u_s, \{rul_i\} >) \xrightarrow{gen} \{< a_s, a_o, rul_i >\}, i = \overline{1..n}$$

При запуске ВМ в СОВ выполняется алгоритм, представленный в виде псевдокода на листинге. При остановке ВМ в СОВ выполняется алгоритм удаления из Rul_{vm} всех ПФ, которые содержат адрес завершаемой ВМ. Представленный алгоритм обеспечивает соответствие ПФ и ПД с учетом состояния $State$.

Листинг. Псевдокод алгоритма генерации ПФ при добавлении ВМ СОВ

НАЧАЛО:
n - адрес запускаемой ВМ
u - пользователь, запускающий ВМ
// генерация ПФ для доступа к сервисам в ВМ
для кажд. vm_i **из** VM **{**
 u_{vm_i} - пользователь vm_i, R_{vm_i} - роли пользователя vm_i
 для кажд. r_j **из** R_{vm_i} **{**
  P_{r_j} - привилении роли r_j
  для кажд. p_k **из** P_{r_j} **{**
   u_{p_k} - пользователь, отвечающий за сервис, описываемый ИВС
   если $u = u_{p_k}$ **тогда** Rul_{vm}+= $gen(vm_i, n, p_k)$
  }
 }

}
// генерация ПФ для доступа из ВМ к сервисам других пользователей
R_u - роли пользователя u
для кажд. r_i **из** R_u **{**
P_{r_i} - привилегии роли r_i
для кажд. p_j **из** P_{r_i} **{**
u_{p_j} - пользователь, отвечающий за сервис, описываемый ИВС
для кажд. vm_k **из** VM **{**
u_{vm_k} - пользователь vm_k
если $u_{vm_k} = u_{p_j}$ **тогда** $Rul_{vm} += gen(n, vm_k, p_j)$
}
}
}
КОНЕЦ.

Выполнение ПД обеспечивается тем, что разработанный метод осуществляет генерацию ПФ для каждой ВМ СОВ, принадлежащей пользователям, которым разрешен доступ к сервисам пользователя запускаемой ВМ, а также ПФ для разрешенного доступа из запускаемой ВМ к сервисам в ВМ других пользователей. Остальное сетевое взаимодействие запрещено.

Третья глава посвящена алгоритмам фильтрации виртуальных соединений в среде облачных вычислений и архитектуре сетецентрической системы РД в СОВ. С точки зрения ПД объекты категории ИВС могут принадлежать классу, в который входят три макросостояния: разрешенные ВС (РВС), запрещенные ВС (ЗВС), неопределенные ВС (НВС). НВС – соединения в данный момент времени разрешенные ПД, но, в рамках которых в дальнейшем может осуществляться запрещенный обмен данными, поэтому они подлежат дальнейшему контролю. НВС соответствует отложенному решению в условиях недостатка доступной информации, например, при установлении транспортного соединения в задачах фильтрации прикладных протоколов. Классификация ИВС сводится к вычислению функции фильтрации виртуального соединения $\mathrm{F(Rules, TBC)}$ для каждого ТВС, формирующего ИВС, область значений которой задана множеством $\{1,0,*\}$, в котором значение функции «1» соответствует РВС, «0» - ЗВС, «*» - НВС. Разработано решение задачи параллельной фильтрации ИВС с использованием современных многоядерных архитектур современных вычислительных систем в виде алгоритма параллельной обработки пакетного трафика, который сохраняет последовательность сетевых пакетов в рамках ТВС и основан на балансировке сетевых пакетов по признаку принадлежности ИВС.

Процесс фильтрации ИВС в МСЭ разделен на две части: определение контекста сетевого трафика и обработка трафика на соответствие ПФ. Первая часть фильтрации выполняется в потоке предварительной обработки и представлена следующим алгоритмом:

1. Инициализация пакетного фильтра, запуск потоков-обработчиков ИВС, количество которых равно количеству ядер микропроцессоров в МСЭ.
2. Ожидание поступления пакета в очередь.
3. Обработка поступившего из очереди пакета – вычисление хеш-функции от параметров заголовков пакета, поиск ИВС в таблице активных соединений, определение потока обработки ИВС. Если в таблице активных соединений отсутствует ИВС, соответствующий пришедшему пакету, то в таблицу вносится запись о новом соединении.
4. Передача пакета в очередь назначенного потока обработчика ИВС.
5. Переход к шагу 2.

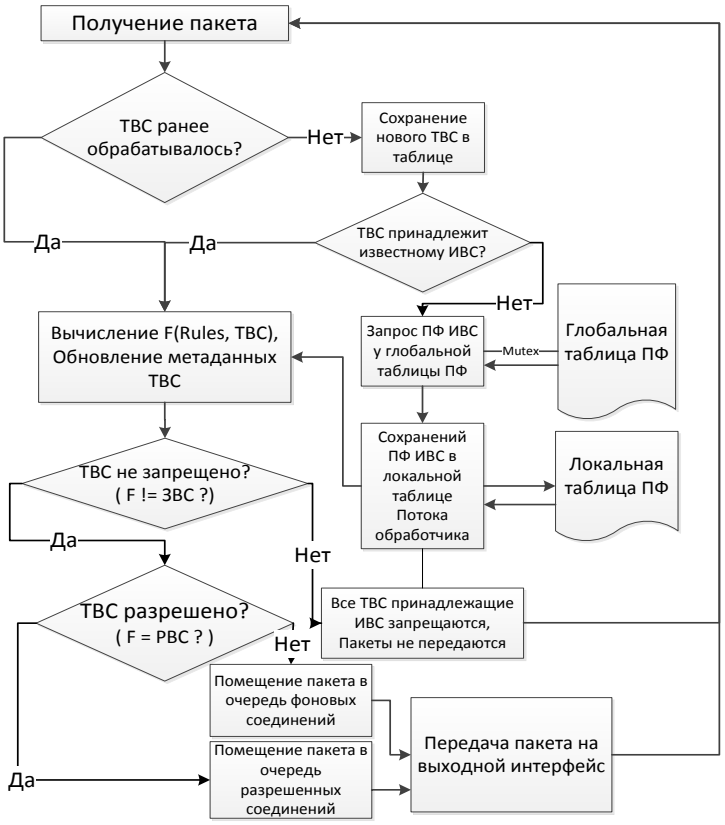

Рисунок 4. Алгоритм обработки ТВС в потоке обработчике

Вторая часть обработки ИВС осуществляется в отдельном потоке-обработчике. Алгоритм фильтрации представлен на рисунке 4. Особенностью алгоритма является загрузка необходимых для обработки ИВС правил фильтрации в локальную память потока, что позволяет уменьшить количество операций синхронизации при обращении к разделяемой между потоками памяти, что повышает скорость работы алгоритма.

Представленные во второй главе категории ИВС и ПФ применены в алгоритме. Поток-обработчик осуществляет обработку ИВС с помощью подмножества ПФ, которое загружено в локальную память потока. При изменении состояния СОВ, объект категории ИВС может измениться. Метод конфигурации ПФ обеспечивает соответствие между объектом категории ИВС и объектом категории ПФ.

Разработана архитектура системы РД в СОВ, с использованием сетецентрического подхода (рисунок 5). В каждом гипервизоре СОВ установлен МСЭ, подключенный к программному виртуальному коммутатору через который взаимодействуют ВМ СОВ. МСЭ осуществляет контроль

сетевого трафика как между ВМ в рамках одного гипервизора, так и между ВМ, функционирующими в разных гипервизорах. Координация действий межсетевых экранов обеспечивается с помощью сервиса управления системой РД, который принимает сообщения об изменении состава ВМ в СОВ через модуль событий сервиса управления СОВ. Полученное сервисом управления системой РД событие об изменении состояния СОВ отправляется в модуль генерации ПФ, который осуществляет генерацию и рассылку ПФ в МСЭ системы РД.

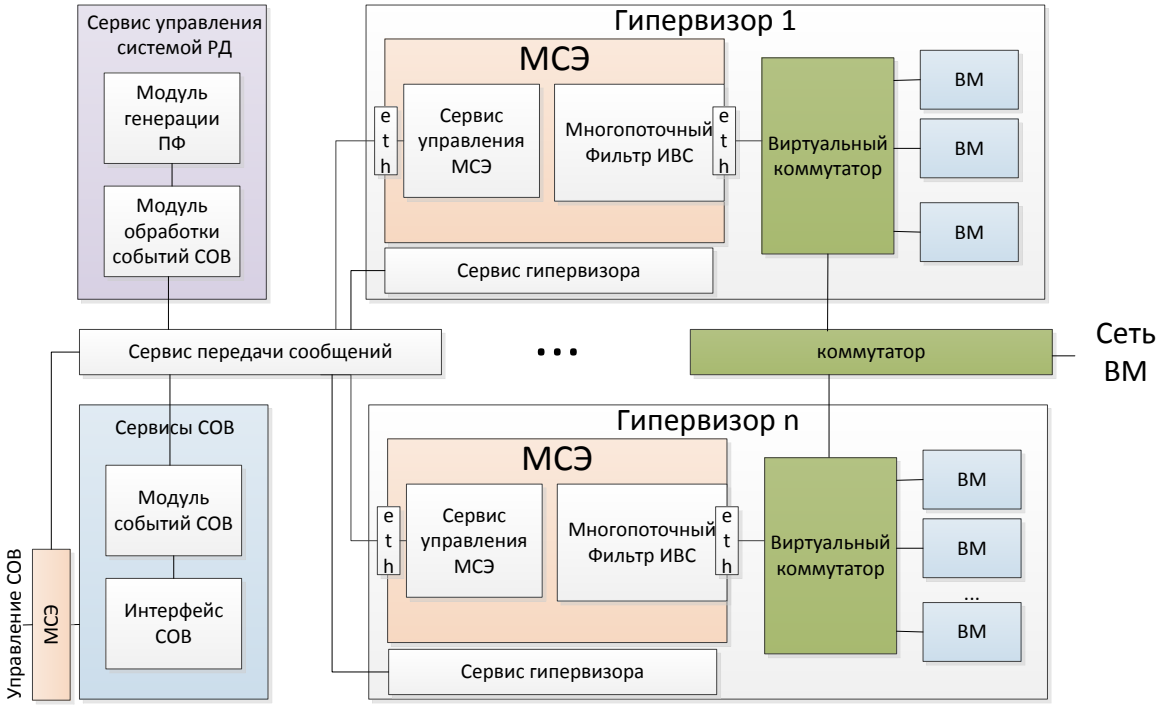

Рисунок 5. Архитектура системы РД в СОВ

В четвертой главе рассмотрены вопросы реализации и практического внедрения полученных результатов. Приведено описание средств РД, являющихся компонентами сетецентрической системы защиты. Для реализации разработанных алгоритмов использована сетевая подсистема Netgraph, функционирующая в ядре сетевой подсистемы операционной системы FreeBSD. Благодаря использованию Netgraph обеспечивается многопоточная обработка виртуальных соединений в контексте ядра, что обеспечило существенный выигрыш в скорости фильтрации (таблица 1) по сравнению с предыдущей реализацией пакетного фильтра в МСЭ ССПТ-2.

Таблица 1. Исследование скорости фильтрации в сети 10Гбит/с

	Параллельный фильтр в ядре ОС	Предыдущая реализация ССПТ-2
Пропускная способность, Гбит/с	9,41	3,25

Исследовано масштабирование скорости фильтрации в многоядерном многопоточном МСЭ. Получен рост скорости фильтрации при изменении количества потоков-обработчиков от одного до четырех в многоядерной системе (таблица 2). Для проведения исследования обработка трафика была искусственно замедлена для наблюдения эффекта в высокоскоростных средах передачи данных.

Таблица 2. Коэффициент увеличения скорости фильтрации при изменении количества потоков в многоядерной платформе МСЭ

	1 ИВС	2 ИВС	3 ИВС	4 ИВС
1 поток	1.0	1,02	1.01	1.0
2 потока	1.0	2.09	2.06	2.6
3 потока	1.0	2.15	3.12	3.12
4 потока	1.0	2.10	3.07	4.14

ПО МСЭ перенесено в виртуальное окружение для гипервизоров XEN, VMware ESX и KVM. С помощью программного коммутатора openvswitch реализовано перенаправление сетевого трафика с ВМ на МСЭ, что обеспечивает контроль информационного взаимодействия между ВМ в рамках одного гипервизора СОВ. Прототипы виртуальных машин с ПО МСЭ экранов машин интегрированы в облачную систему, построенную на базе IaaS платформы OpenStack. Разработанные алгоритмы использованы при создании программного обеспечения МСЭ ССПТ-2, сертифицированного по требованиям ФСТЭК и ФСБ для применения в современных высокоскоростных компьютерных сетях.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Разработана модель информационного взаимодействия для описания процессов разграничения доступа к информационным сервисам, учитывающая динамические характеристики среды облачных вычислений. Для формализации соответствия между ИВС и ПФ, необходимыми для контроля информационного обмена, осуществляемого в рамках рассматриваемого ИВС, и учета динамических характеристик СОВ применен формализм теории категорий.
2. Разработан метод конфигурации межсетевых экранов, основанный на динамическом формировании правил фильтрации в соответствии с изменяющимися параметрами информационного взаимодействия. Метод позволяет оперативно реагировать на изменение состояния СОВ.

3. Разработан параллельный алгоритм фильтрации виртуальных соединений, который позволил существенно повысить скорость фильтрации ИВС и использовать вычислительные ресурсы СОВ за счет многопоточной обработки пакетного трафика.
4. Разработана архитектура системы защиты информационного взаимодействия, обеспечивающей выполнение заданной политики доступа. Система защиты состоит из межсетевых экранов, функционирующих в виртуальных машинах и сервиса управления, осуществляющего конфигурацию МСЭ при изменении состояния СОВ.

СПИСОК ОСНОВНЫХ ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

1. **Лукашин, А.А. Система контроля доступа в среде облачных вычислений [Текст] / В.С. Заборовский, А.А. Лукашин // Научно-технические ведомости СПбГПУ. Информатика, Телекоммуникации, Управление. №4 (152) 2012. – СПб.: Изд-во Политехн. Ун-та, 2012. С. 7-12.**
2. **Лукашин, А.А. Сетецентрическая модель и методы контроля доступа к информационным ресурсам в среде облачных вычислений [Текст] / В.С. Заборовский, А.А. Лукашин // Научно-технические ведомости СПбГПУ. Информатика, Телекоммуникации, Управление. №2 (145) 2012. – СПб.: Изд-во Политехн. Ун-та, 2012. С. 91-95**
3. **Лукашин, А.А. Архитектура сервиса для решения ресурсоемких задач в распределенной вычислительной среде [Текст] / Лукашин А.А., Лукашин А.А., Тютин Б.В., Котляров В.П. // Научно-технические ведомости СПбГПУ. Информатика, Телекоммуникации, Управление. №4 (128) 2011. – СПб.: Изд-во Политехн. Ун-та, 2011. С. 146-149.**
4. **Лукашин, А.А. Архитектура системы разграничения доступа к ресурсам гетерогенной вычислительной среды на основе контроля виртуальных соединений [Текст] / Заборовский В. С., Лукашин А. А., Купреенко С. В., Мулюха В. А. // Вестник УГАТУ. Управление, вычислительная техника и информатика, Т.15 № 5 (45) 2011 г. – Уфа: Изд-во Уфимского авиационного технического университета, 2011. С. 170–174.**
5. Лукашин, А.А. Архитектура системы разграничения доступа к ресурсам гетерогенной вычислительной среды на основе контроля виртуальных соединений [Электронный ресурс] / В.С. Заборовский, А.А. Лукашин, С.В. Купреенко, В.А. Мулюха. // Параллельные вычислительные технологии (ПаВТ’2011), 2011, С. 495–500. Режим доступа: http://omega.sp.susu.ac.ru/books/conference/PaVT2011 (дата обращения 01.09.2012).

6. Лукашин, А.А. Многоядерная вычислительная платформа для высокопроизводительных межсетевых экранов [Текст] / Заборовский В.С., Лукашин А.А., Купреенко С.В. // Высокопроизводительные вычислительные системы. Материалы Седьмой Международной научной молодежной школы. – Таганрог: Изд-во ТТИ ЮФУ, 2010. 336 с.
7. Лукашин, А.А. Методы и средства передачи управляющих сообщений в ядро ОС FreeBSD при решении задач фильтрации пакетного трафика [Текст] / Лукашин А.А. Якименко А.В. // XXXIX неделя науки СПбГПУ, Материалы Всероссийской межвузовской научно-технической конференции студентов и аспирантов, 6-11 декабря 2010 года, Часть XV, факультет при ЦНИИ робототехники и технической кибернетики. – СПб.: Изд-во Политехнического университета, 2010. С. 5-7.
8. Lukashin, A.A. Dynamic Access Control Using Virtual Multicore Firewalls [Текст] / Alexey Lukashin and Vladimir Zaborovsky // The Fourth International Conference on Evolving Internet INTERNET 2012, ISBN: 978-1-61208-204-2, 2012, pp. 37-43.
9. Lukashin, A.A. Dynamic Access Control in Cloud Services [Текст] / Vladimir Zaborovsky, Alexey Lukashin, Sergey Kupreenko and Vladimir Mulukha // IEEE International Conference on Systems, Man and Cybernetics, 2011, pp. 1400-1404.
10. Lukashin, A.A. Access Isolation Mechanism Based On Virtual Connection Management In Cloud Systems [Текст] / Alexey Lukashin, Vladimir Zaborovsky and Sergey Kupreenko // 13th International Conference on Enterprise Information Systems (ICEIS 2011), 2011, pp. 371 – 375.
11. Lukashin, A.A. Dynamic Access Control in Cloud Services [Текст] / Vladimir Zaborovsky, Alexey Lukashin, Sergey Kupreenko and Vladimir Mulukha // International Transactions on Systems Science and Applications, ISSN 1751-1461, Vol. 7, No. 3/4, 2011, pp. 264-277.