На правах рукописи

МОЛЯКОВ Андрей Сергеевич

СРЕДСТВА ПРОТИВОДЕЙСТВИЯ СКРЫТЫМ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 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 – 2014

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский государственный политехнический университет».

Научный руководитель: Заборовский Владимир Сергеевич,

доктор технических наук, профессор, заведующий кафедрой «Телематика (при ЦНИИ РТК)» ФГАОУ ВО «Санкт-Петербургский государственный политехнический университет»

Официальные оппоненты: Воробьев Владимир Иванович,

доктор технических наук, профессор, заведующий лабораторией информационно-вычислительных систем Санкт-Петербургского института информатики и автоматизации РАН

Гугель Юрий Викторович,

кандидат технических наук, доцент, директор Санкт-Петербургского филиала ФГАУ ГНИИ ИТТ «Информика»

Ведущая организация: Федеральное государственное автономное научное учреждение «Центр информационных технологий и систем органов исполнительной власти» Министерства образования и науки РФ (ЦИТиС), г. Москва

Защита состоится «23» декабря 2014 г. в на заседании диссертационного совета Д212.229.27 при ФГАОУ ВО «Санкт-Петербургский государственный политехнический университет» по адресу 195251,Санкт-Петербург, ул. Политехническая, 29, ауд. 175 главного здания.

С диссертацией можно ознакомиться в библиотеке и на сайте http://www.spbstu.ru/science/defences.html ФГАОУ ВО «Санкт-Петербургский государственный политехнический университет».

Автореферат разослан**:** « » 2014 г.

Ученый секретарь
диссертационного совета Платонов Владимир Владимирович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертации

Стремительное развитие технологий виртуализации и облачных вычислений формирует новые источники угроз информационной безопасности, которые часто носят скрытый характер, что необходимо учитывать при создании нового поколения систем кибербезопасности. Так использование недекларированных возможностей системного программного обеспечения для организации компьютерных атак, направленных на модификацию программных кодов или подмену субъектов и объектов информационного обмена, значительно снижает эффективность применения традиционных средств защиты от нарушений конфиденциальности, целостности и доступности ресурсов. Поэтому контроль процессов и потоков данных в среде облачных вычислений, включая процедуры инициализации на всех уровнях взаимодействия, в том числе и на уровне гипервизора, становится неотъемлемым средством противодействия скрытым для гостевых операционных систем (ОС) угрозам информационной безопасности.

Актуальность разработки технологии противодействия попыткам внешних и внутренних нарушителей изменить состояние защищенности информационных ресурсов в среде облачных вычислений отмечается многими российскими и зарубежными учёными, в том числе В.А. Курбатовым, П.Д. Зегждой,А.А. Грушо,В.Ю. Скибой, Н.А. Гайдамакиным, А.А. Гладких, В.С. Заборовским, С. Воглом, Р. Сэйлером, Ф. Мортинелли, Дж. Рутковской и др. В их работах большое внимание уделяется разработке методов и средств защиты информации, в которых учитываются особенности виртуализации аппаратных ресурсов и системного программного обеспечения (ПО), существенно влияющих на состояние защищенности используемых программных сервисов.

Перспективным направлением совершенствования систем защиты информации в среде облачных вычислений является разработка новых средств противодействия, основанных на контроле процессов выделения ресурсов в соответствии с результатами оперативной идентификации потенциальных уязвимостей, возникающих как на уровне процессов контроля доступа к прикладным информационным сервисам гостевых ОС, так и на уровне системных вызовов гипервизоров. Сложность этой задачи связана с тем, что в среде облачных вычислений выделение ресурсов носит динамический характер, и в зависимости от состояний субъектов и объектов информационного взаимодействия порождаемые ими системные вызовы на выделение ресурсов могут становиться источниками различных видов разрушающих воздействий. Отмеченные особенности часто учитываются нарушителями для организации атак на подсистемы гипервизора, отвечающих за планирование задач и верификацию команд на соответствие требованиям политики безопасности. Такие угрозы необходимо не только оперативно выявлять, но и эффективно блокировать каналы информационных воздействий, которые используются для нарушения функционирования приложений и системного ПО. Для создания средств защиты от угроз, недоступных для выявления со стороны гостевых ОС, требуется разработка новых моделей угроз, которые учитывают свойства операций выделения системных ресурсов, соответствие выполняемых транзакций требованиям политики безопасности, а также механизмы контроля контекста взаимодействия системных процессов, реализуемых в ОС виртуальных машин и гипервизоре. Под понятием «*транзакция*» в работе понимается завершенный *процесс* обработки запросов гостевых ОС на выделение ресурсов, включая контекст выполняемых операций.

С учетом вышесказанного, противодействие угрозам информационной безопасности, направленных на модификацию программных кодов, подмену субъектов и объектов информационного обмена, нарушение целостности и доступности ресурсов,

блокирование доступа и навязывание ложной информации, является актуальной научно-технической задачей, решению которой посвящена данная диссертационная работа.

Целью исследования является разработка средств противодействия скрытым угрозам информационной безопасности в среде облачных вычислений, учитывающих архитектуру гипервизора и особенности современных технологий виртуализации аппаратных ресурсов.

Для достижения поставленной цели в диссертационной работе были решены следующие задачи:

1. Разработана модель скрытых угроз информационной безопасности, учитывающая контекст выполнения операций информационного взаимодействия в среде облачных вычислений.
2. Разработана модель операций, выполняемых над данными при их обработке в среде облачных вычислений, позволяющая формализовать описание информационных процессов в виде мультиграфа транзакций.
3. Разработан метод противодействия скрытым угрозам, основанный на контроле запросов на выделение ресурсов в соответствие с оценкой безопасности выполняемых транзакций.
4. Разработан алгоритм предикативной идентификации угроз, возникающих для подсистем гипервизора при реализации запросов гостевых ОС на выделение информационных ресурсов.
5. Создан опытный образец программного обеспечения «Альфа - монитор» и проведена его успешная апробация в среде облачных вычислений**.**

Методы исследования: для решения сформулированных задач использовался аппарат теории графов, теории алгоритмов, теории вероятностей, методы защиты информации и компьютерного реверс-инжиниринга.

Объект исследования: скрытые угрозы информационной безопасности в среде облачных вычислений.

Предмет исследования: модели, методы и алгоритмы обнаружения скрытых угроз на уровне гипервизора среды облачных вычислений и гостевых операционных систем виртуальных машин (ВМ).

Научная новизна работы состоит в применении теории графов и методов декомпозиции иерархических структур для формализации процессов информационного взаимодействия и построении модели операций противодействия скрытым угрозам в среде облачных вычислений с учетом архитектуры гипервизоров и особенностей современных технологий виртуализации аппаратных ресурсов.

Положения, выносимые на защиту:

1. Модель скрытых угроз информационной безопасности, основанная на декомпозиции динамических процессов взаимодействия субъектов и объектов среды облачных вычислений.
2. Модель операций в виде мультиграфа процессов, формируемых в среде облачных вычислений с учетом атрибутов объектов и контроля параметров субъектов информационного взаимодействия.

3. Метод противодействия скрытым угрозам в среде облачных вычислений, основанный на формализации транзакций и контроле процессов выделения ресурсов для гостевых ОС, отвечающих требованиям выбранной политики безопасности.

4. Алгоритм идентификации скрытых угроз, основанный на предикативном анализе мультиграфа процессов и верификации команд, выполнение которых не нарушает требований безопасности на уровне процессов гостевой ОС и гипервизора среды облачных вычислений.

Обоснованность и достоверность представленных в диссертационной работе научных положений обеспечивается учетом особенности современных технологий виртуализации, корректностью использования аналитического аппарата и апробацией полученных результатов в печатных трудах и докладах на всероссийских и международных научных конференциях.

Практическая значимость работы. Результаты исследований, полученные в ходе выполнения диссертационной работы, были успешно апробированы автором при создании VIPNet OfficeFirewall 3.0, при разработке программного комплекса «Альфа-монитор», при выполнении ряда договорных научно-исследовательских работ со стороны заказчика (ФГУП НИИ «Квант», НПО РУСНЕТ, НПО ФРАКТЕЛ), а также в учебном процессе и научных исследованиях на кафедре «Телематика (при ЦНИИ РТК)» ФГАОУ ВО «СПбПУ» по дисциплинам «Сети ЭВМ и телекоммуникаций» и «Методы и средства защиты компьютерной информации».

Апробация и публикация результатов работы.

Основные результаты исследования обсуждались на семинаре «Проблемы современных информационно-вычислительных систем», Москва, 2014 г.; на Общероссийской научно-технической конференции «Информационная безопасность регионов России», Санкт-Петербург, 2013 г.; на международной научно-технической конференции СИТ, г. Пенза, 2009 г.; на XXXVII научной и учебно-методической конференции СПбГУ ИТМО, Санкт-Петербург, 2008 г.; на 9 Международной научно-практической конференции, Таганрог, 2008 г.; на IV межвузовской конференции молодых ученых, Санкт-Петербург, 2007 г.; на XI научно-практической конференции «Теория и технология программирования и защиты информации», Санкт-Петербург, 2007 г.; на научно-технической конференции «День антивирусной безопасности», Санкт-Петербург, 2007 г

Основные результаты и положения работы опубликованы в 20 научных статьях, в том числе 12 статей в изданиях, входящих в перечень Высшей аттестационной комиссии Министерства образования и науки Российской Федерации**.**

Структура и объем диссертационной работы. Диссертационная работа объемом 137 машинописных страниц содержит введение, четыре главы и заключение, список литературы, содержащий 76 наименований, и 2 приложения. Общий объём работы – 137 страниц, 20 рисунков и 13 таблиц.

СОДЕРЖАНИЕ ДИССЕРТАЦИИ

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

В первой главе представлен обзор основных методов и моделей противодействия угрозам информационной безопасности в среде облачных вычислений. Проведен анализ существующих угроз, реализуемых с использованием недекларированных возможностей программного обеспечения (ПО). Показано, как реализация скрытых для гостевых ОС угроз позволяет вредоносному коду маскироваться под системный процесс, нанося ущерб безопасности среды облачных вычислений посредством блокирования, хищения, уничтожения или несанкционированной передачи информации.

Особое внимание уделено анализу недостатков современных технологий защиты информации в среде облачных вычислений, которые не учитывают динамический характер предоставляемых прикладных и системных программных сервисов. Показано, как облачные системы класса «инфраструктура как сервис» могут стать источником угроз нарушения безопасности программного обеспечения, что связано с активным характером взаимодействия субъектов и объектов доступа, приводящим к рискам нарушения целостности и доступности программных сервисов, предоставляемых в режиме удаленного доступа. Отмечено, что особую опасность предоставляют угрозы, которые реализуются внутри периметра безопасности компьютерной сети, так как их локализация с применением современных средств защиты информации (СЗИ), например, антивирусов и сканеров безопасности, встречает существенные трудности. Поэтому для создания эффективных механизмов защиты ПО в среде облачных вычислений требуется разработка новых моделей угроз и создание методов отражения компьютерных атак, которые позволяют оперативно идентифицировать скрытые и потенциально опасные процессы информационного взаимодействия. На основе проведенного анализа и оценки влияния новых угроз на состояние защищенности ресурсов среды облачных вычислений в главе определена цель диссертационного исследования и сформулирован перечень научно-технических задач, решение которых обеспечивает ее достижение.

Во второй главе разработана модель скрытых угроз, в которой учитывается динамический характер субъектов и объектов информационного взаимодействия, а также контекст выполнения операций информационного взаимодействия в среде облачных вычислений. Автором предложена 8 – уровневая иерархическая структура для разработки средств противодействия скрытым для гостевых ОС угрозам информационной безопасности с учетом современных технологий виртуализации и архитектуры гипервизоров xen и kvm. Для формализации описания рассматриваемых процессов предложена модель операций, выполняемых на разных уровнях функционирования среды облачных вычислений. В предложенной модели операций различные компоненты гипервизора рассматриваются в качестве потенциального источника угроз информационной безопасности, которые реализуется путем распространения вредоносного программного обеспечения или инициализации процессов, нарушающих состояние защищенности ресурсов среды облачных вычислений. С помощью разработанной модели предложено формализованное описание угроз, которые формируют последовательности некорректных запросов к программным модулям гипервизора или используют недекларированные возможности системного и прикладного ПО. Эти последовательности позволяют классифицировать операции, которые используют злоумышленники для реализации скрытых угроз информационной безопасности в среде облачных вычислений. Предложено описание операций, которое позволяет идентифицировать системные вызовы гостевых ОС с целью «встраивания» вредоносных программных кодов в среду исполнения на уровне планировщика задач и диспетчера работы с оборудованием.

Предложенный в главе подход к описанию операций основан на классификации рисков нарушения информационной безопасности и анализе контекста выполнения потоков команд, посредством которых могут передаваться данные в обход требований

принятой политики безопасности, что приводит нарушению защищенности ресурсов гипервизора. В разработанной модели носителями анализируемых операций являются множества объектов и субъектов доступа, которым присвоены различные уровни безопасности. Для контроля уровня безопасности операций порождения новых субъектов, а именно операции *Create* $(Sub_i, O_m) \rightarrow Sub_j$, предлагается использовать признак неизменности объекта, порождающего субъект доступа. Этот признак должен выполняться для момента времени $t>t_0$, где t_0 – момент активизации операция, тогда порождение нового субъекта с номером jстановится возможным только при выполнении условия $O_m[t] = O_m[t_0]$, где Subj – субъект доступа, O_m – объект доступа, j, m – номера объектов в предложенной спецификации рассматриваемой облачной среды.

Для расширения функциональности в разработанной модели операций введено четыре уровня привилегий команд, а именно: Priv0 - уровень привилегий команд процессора, Priv1 – уровень привилегий ядра ОС, Priv2 – уровень привилегий администратора безопасности сервера виртуализации, Priv3 – уровень привилегий пользователей. С учетом того, что существенной особенностью операций в среде облачных вычислений является возможность изменения роли субъектов и объектов информационного взаимодействия, для контроля неизменности объектов предлагается использовать специальные механизмы идентификации контекста выполнения процессов. В результате любой инициатор процесса доступа может использовать только разрешенные последовательности операций, признак которых задается в виде логической функции, которая определена на кортежах значений трех переменных:

$$\mathbf{Pi= (s, Ord, Context\_type),} \qquad \mathbf{(1)}$$

s – предикат, определяющий контекст выполнения процесса в соответствии с условиями:

$$s = \begin{cases} 0, \text{ если } \max(Privi, Privj) = Privj, \text{ повышение уровня привилегий;} \\ 1, \text{ если } \min(Privi, Privj) = Privj, \text{ понижение уровня привилегий;} \end{cases}$$

Выражение max(Privi, Privj) означает выбор максимального значения из Privi и Privj, min(Privi, Privj) – минимального значения, Privi – уровень привилегий доступа в Ri состоянии, Privj – уровень привилегий доступа в Rj состоянии. Если предикат s в (1) равен 0, то процесс (поток) получает статус System, то есть описывает объект, которому делегирован в среде облачных вычислений максимальный уровень полномочий (возможность выполнять привилегированные команды процессора), а если предикат s равен 1, то процессу (потоку) приписывается статус обычного приложения.

В свою очередь, предикат Ord задает признак родительского или дочернего процесса (потока):

$$Ord = \begin{cases} 0, \text{ процесс или поток родительский;} \\ 1, \text{ в противном случае;} \end{cases}$$

Множеством значений переменной *Context_type* является трит{1,0, –1}, который характеризует контекст выполнения операций. Так, при Context_type = 1 разрешены операции чтения или записи в область памяти приложений; при Context_type = 0 реализуется режим ожидания новых транзакций, при этом не осуществляются операции

записи данных; при Context_type = –1 разрешены операции чтения или записи в привилегированную область памяти гостевой ОС.

С использованием введенных обозначений модель функционирования гипервизора может быть представлена конечным автоматом вида:

$$\mathbf{mod_i = (Ei, Ri, start, Privi, Fi, Pi, Vi)}, \quad (2)$$

где $mod_i \in \mathbf{M}$ – множество всех компонентов среды взаимодействия процессов**;** переменные Ei и $\mathbf{V}i \in \mathbf{E}$ – задают множество событий или входных воздействий, изменяющих состояния гипервизора, переменная start – задает начальное состояние виртуальной машины, переменная Privi – уровень привилегий в Ri состоянии; **P**i : Ri → {1|0}, **P**i – логическая функция оценки допустимости состояния, указанная в формуле (1); отображение **Fi**: Rix**V**i → Rj – задает функцию перехода из состояния Ri вRj под внешним воздействием**V**i.

Внешние воздействия **V**i представляют собой запросы пользователей ВМ, поступающие на обработку в гипервизор, или процессы вредоносного ПО, модифицирующие компоненты гипервизора.

Предложенная модель операций позволяет оперативно построить отображение Ri → {1|0}как конъюнкцию простых предикатов, характеризующих состояния компонентов гипервизора. Для разрешенных состояний гипервизора формализованное описание операций порождения субъектов или объектов доступа может быть представлена в следующем виде: *Create* $(Sub_i, O_m, s, Ord, Context\_type) \rightarrow Sub_j$, *Create* $(O_m, s, Ord, Context\_type) \rightarrow O_l$.При этом таблицы разрешенных связей объектов и субъектов доступа, с помощью которых осуществляется контроль транзакций порождения новых объектов, могут быть расширены за счет состояний, порождающих скрытые угрозы.

В результате предикативная функция идентификации скрытых угроз может быть представлена как отображение 8-уровневой модели операций на множество его возможных состояний, состоящее из опасных, безопасных и неопределенных подмножеств. Поэтому модель скрытых угроз описывается в виде расширенного кортежа:

$$\mathbf{< Source, Services, Devices, \{proc\}, Actions, \{hv\}, \{vm\}, SecurityRoles >}, \quad (3)$$

- Source – субъект доступа или процесс источник угрозы;
- Services – набор шаблонов политик безопасности (ПБ), используемых традиционными СЗИ(например, правила фильтрации для межсетевых экранов и пр.);
- Devices – список устройств, установленных на серверах виртуализации и используемых гостевыми операционными системами ВМ (диск, сетевой контроллер и т.п.), как объекты доступа;
- {proc} – множество субъектов воздействия (вредоносный код гипервизора и.т.п.);
- Actions – список операций субъекта, выполняемых с ресурсами объекта доступа (выполнение команд read, write, append,create, execute, delete и т.п.);
- {hv} – подмножество компонентов mod_i, представляющее процессы информационного взаимодействия;
- {vm} – объекты воздействия (например, множество виртуальных машин).
- Security-Roles – процедуры ролевой политики безопасности, используемые для противодействия скрытым угрозам, реализуемые в виде набора меток

безопасности, которые представляют собой кортеж значений трех переменных формулы (1).

В конце второй главы предложено расширение модели угроз, описывающей уязвимости гипервизора с учетом состава и направленности операций, реализуемых в рамках схемы информационного взаимодействия «субъект-действие-объект». Показано, что динамический характер субъектов и объектов порождает новый класс угроз, в которых злоумышленник (субъект) атакует сервер виртуализации (объект), модифицируя отдельные компоненты гипервизора (таблица 1).

Таблица 1. Перечень угроз, влияющих на безопасность гипервизора

Название	**Возможные последствия**
Нестандартное выполнение команд ВМ в гипервизоре	Получение несанкционированного доступа к ресурсам гипервизора
Нарушение однозначности переходов состояний при информационном обмене между ВМ и гипервизором	Получение несанкционированного доступа к данным пользователя, расположенным на разных виртуальных машинах
Модификация программных компонентов гипервизора	Распространение вредоносного ПО в среде облачных вычислений

При этом модифицированные гипервизоры, установленные на серверах виртуализации, которые находятся в одной или разных подсетях, становятся скрытыми участниками компьютерной атаки (субъектами доступа), а выполняемые под их управлением прикладное программное обеспечение пользователей – объектами доступа.

Предложено процессы взаимодействия в гипервизоре декомпозировать на 8-уровневую иерархическую структуру (рис. 1).

На рис. 1 используются следующие обозначения: R_i, i = 1...8 – состояния процессов; S1 – уровень приложений; S2 – уровень ядра гостевой ОС; S3 – уровень обработчиков прерываний; S4 – уровень менеджера памяти гипервизора; S5 – уровень подсистемы – ввода вывода гипервизора; S6 – уровень планировщика задач гипервизора; S7 – диспетчер работы с оборудованием гипервизора; S8 – уровень исполнительного процессора. На уровнях S1– S5 функционируют традиционные СЗИ, которые используют наборы правил контроля доступа, отвечающих требованиям политики безопасности. На уровнях S6 – S7 реализуются скрытые для гостевых ОС угрозы, а на уровне S8 осуществляется контроль выполнения операций.

Левыми стрелками p1, p2, p3, p4, p5, p6, p7 обозначены переходы в мультиграфе транзакций без изменения контекста выполнения операций. Правыми стрелками q1, q2, q3, q4, q5, q6, q7 обозначены переходы с изменением контекста выполнения операций, когда компонент mod_i модифицирован вредоносным ПО.

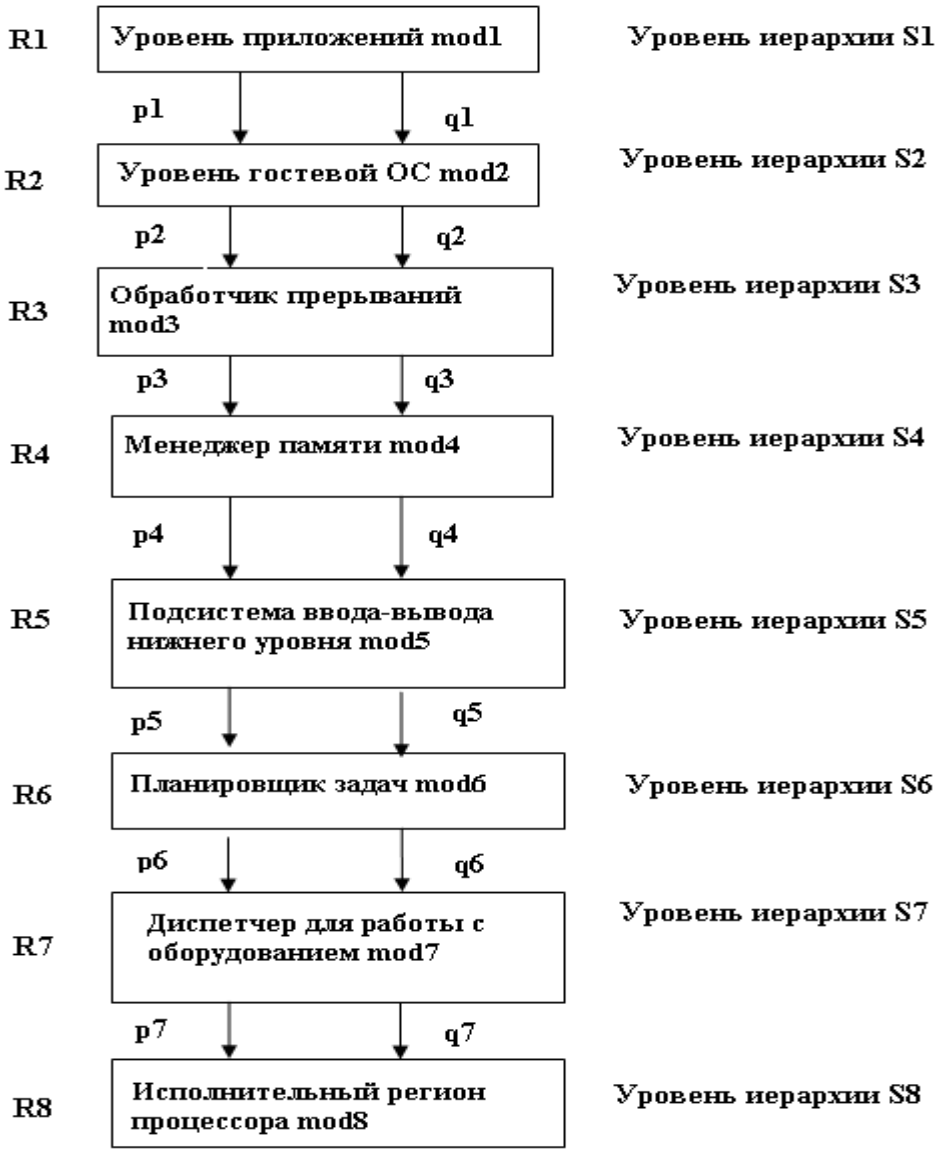

Рисунок 1 Мультиграф транзакций

На основе предложенной декомпозиции модель операций можно конструктивно представить с помощью мультиграфа транзакций, который описывает разрешенные механизмы инициализации процессов доступа к прикладным и системным информационным ресурсам. В результате предложенной формализации описание скрытых угроз сводится к введению контекстно-зависимых переходов в мультиграфе транзакций, поэтому для их выявления требуется разработка эффективных алгоритмов идентификации состояния как прикладных, так и системных процессов.

Для разработанной модели операций условие разрешимости задачи противодействия скрытым угрозам сформулировано в виде теоремы 1:

Теорема 1. Необходимым условием разрешимости задачи противодействия скрытым угрозам в среде облачных вычислений является наблюдаемость переходов состояний в мультиграфе транзакций.

В работе показано, что наблюдаемость переходов мультиграфа требует их представления в виде набора простых предикатов или их конъюнкции.

Основным теоретическим результатом второй главы диссертации является формализация процессов формирования скрытых угроз информационной безопасности, в которых учитывается динамический характер выделения информационных ресурсов и контекста выполняемых операций в среде облачных вычислений.

Так как носителем состояний гипервизора, является множество событий **E**, которое состоит из двух непересекающихся подмножеств: Ehv – множества событий, возникающих на уровне гипервизора, множество Evm – множество событий, генерируемых виртуальными машинами vm, в том числе запросы пользователей на изменение сценариев конфигураций запускаемых ВМ {conf}, то нарушитель может использовать для организации атаки события, генерируемые виртуальными машинами посредством «встраивания» вредоносных операций на нижние уровни иерархии среды выполнения команд, которые не контролируются традиционными СЗИ. Такие действия реализуются посредством каналов межпроцессного обмена, изменяющего контекст выполнения операций, что позволяет злоумышленнику менять последовательность переходов с одного функционального уровня модели гипервизора на другой. На рисунке 2 приведен пример перехвата системного вызова гостевых ОС на уровне гипервизора с учетом возможности возникновения скрытых угроз безопасности для информационных ресурсов виртуальных машин ВМ1 и ВМ2. Принимая во внимание структуру взаимодействия системных и прикладных процессов (рис.1),переходы между всеми состояниями гипервизора можно описать с помощью мультиграфа транзакций, а именно G= <R, D, I>, где состояния гипервизора Ri представляют вершины мультиграфа, а ребра Di – возможные переходы между этими состояниями; I – матрица инциденций мультиграфа. Как видно из рисунка 2, компоненты гипервизора могут модифицироваться вредоносным ПО в результате атак внутреннего нарушителя с помощью перехвата данных модулями вредоносного ПО. На рисунке 2 стрелками 1 обозначено прохождение запроса от ВМ1 к гипервизору, стрелками 5 – прохождение запросов от ВМ2 к гипервизору. Стрелками 3 показаны каналы перехвата данных модулями вредоносного программного обеспечения, например IceBrute, RuStock, DRM, Croax, Red Dragon, BluePill, VICE Toolkit, которое модифицируют данные, полученные от пользователя ВМ1 (стрелки 2), отправляя их (стрелка 4) с использованием штатного драйвера для работы с устройством (например, диск, сетевой контроллер и т.п.), нарушает безопасный режим работы ВМ2. Так как современные СЗИ функционируют на более высоких уровнях взаимодействия процессов в среде выполнения команд (уровни S1– S4), поэтому они не могут блокировать действия вредоносного программного обеспечения на уровнях S5–S7.

Разработанное описание информационных процессов на основе мультиграфа транзакций позволяет контролировать соответствие выполняемых операций требованиям безопасности и задает признаки (критерии), по которым идентифицировать их состояние на всех уровнях модели операций, что открывает новые возможности обнаружения и блокирования последствий разрушающих воздействия от явных и скрытых угроз нарушения информационной безопасности в среде облачных вычислений.

Рисунок 2 Пример перехвата системного вызова гостевой ОС на уровне гипервизора

В третьей главе предложен метод обнаружения скрытых угроз с использованием мультиграфа транзакций, разработан и реализован алгоритм идентификации скрытых угроз, основанный на предикативном анализе мультиграфа транзакций и верификации команд, выполнение которых не нарушает требований безопасности на уровне процессов гостевой ОС и гипервизора. С этой целью введено понятие «контекст выполнения переходов», который представляется в виде дерева реберных графов для каждого узла мультиграфа транзакций.

Разработанный метод основан на том, что набор меток {m} для «раскрашивания» мультиграфа транзакций представляется кортежем значений трех переменных формулы (1). Изменение контекста выполнения операций формализуется в виде матрицы инциденций гипервизора.

Неоднозначность переходов между узлами мультиграфа транзакций объясняется существованием неконтролируемых состояний гипервизора. Однако, как показано в главе 2, связанные с этими состояниями функции предикатов разрешимы для всех наборов контролируемых переменных. Поэтому наряду с описанием информационных процессов с помощью мультиграфа транзакций для каждого отдельного процесса можно построить граф порожденных им процессов, которые связаны общим идентификационным номером Context_idи наборами меток. Алгоритм идентификации скрытых угроз информационной безопасности может быть представлен следующей последовательностью шагов:

Шаг 1. Построить мультиграф транзакций.

Шаг 2. Представить контекст выполнения запроса в виде набора меток {m}.

Шаг3. Провести анализ корректности завершения команд с точки зрения требований информационной безопасности.

Требования политики безопасности формулируются в терминах, которые задают последовательность обработки операций и ограничений на возможность повышения привилегий процессов модели, представленной на рисунке 1. При этом на каждом уровне модели операций S1–S8 ведется протоколирование событий и результатов, включая параметрыT – время и Res – результат выполнения операций, а мультиграф транзакций «раскрашивается» с помощью набора меток. Ограничение на повышение привилегий и контроль переходов при изменении контекста операций задаются значениями логической функции оценки допустимости состояний (1), а контроль выполнения потоков, порождаемых субъектами доступа, реализуется на основе принципа наименьших привилегий (табл. 2).

Таблица 2. Таблица правил политики безопасности

Поле s	***Поле Ord***	***Поле Context_type***	***Действия, отвечающие требованиям политики безопасности***
0	*X*	*-1*	Запретить состояния, так как осуществляется попытка повредить компоненты гипервизора со стороны злоумышленника за счет перехвата обращений пользователей ВМ к драйверам устройств
0	*X*	*1*	Запретить состояния, так как осуществляется попытка злоумышленника изменить данные о конфигурации ВМ
1	*X*	*X*	Разрешить состояния
0	*0*	*0*	Ожидание запросов пользователей и их регистрация

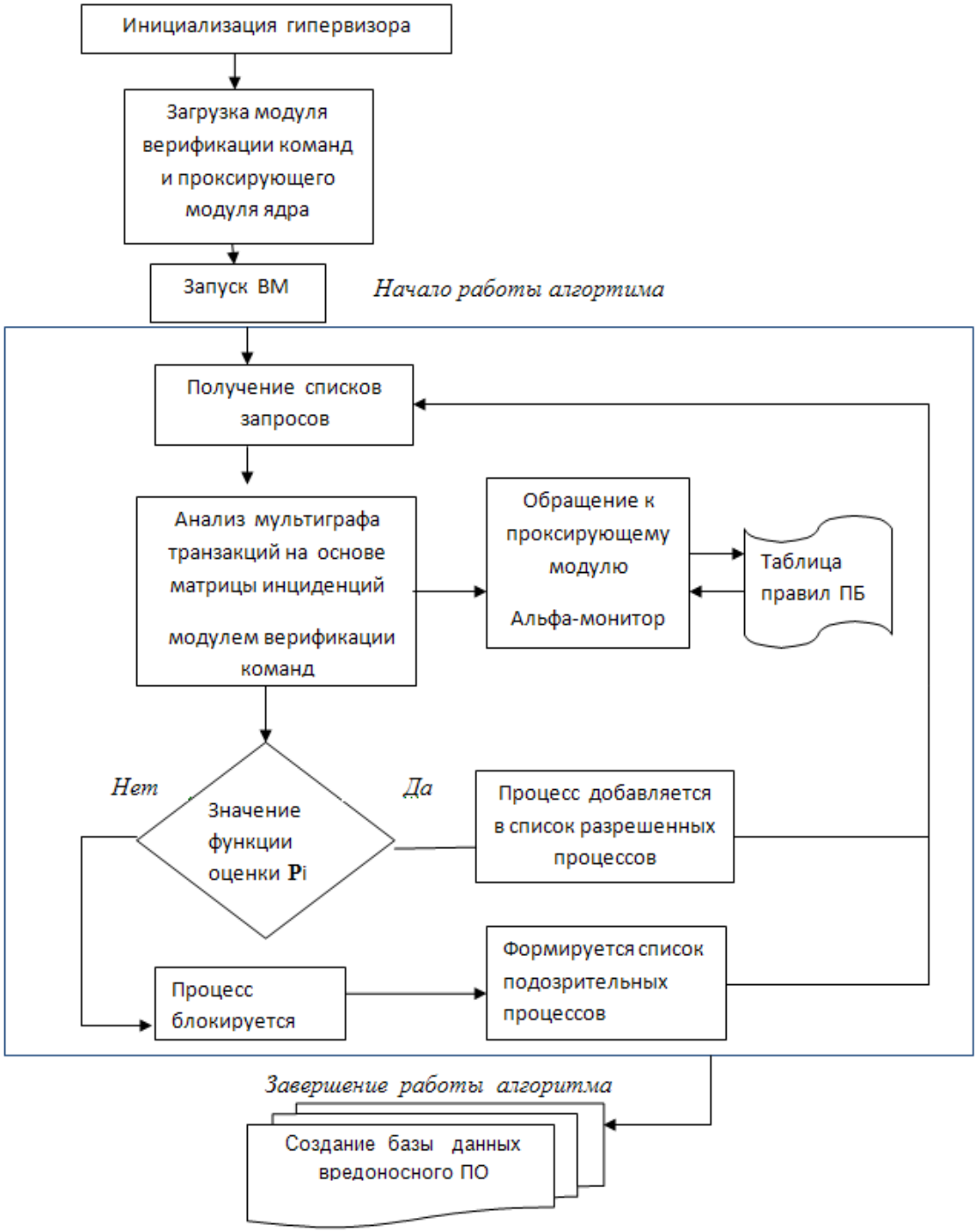

Рисунок 3 Схема работы алгоритма предикативной идентификации скрытых угроз

На рисунке 3 приведена схема работы алгоритма идентификации скрытых угроз в среде облачных вычислений. Показано, что алгоритм идентификации позволяет обнаружить вредоносное программное обеспечение в компонентах гипервизора и гостевых ОС, когда в качестве входных параметров используются списки запросов от пользователей виртуальных машин, которые представляются определенным набором операций.

Алгоритм учитывает особенности функционирования программных эмуляторов устройств, которые обрабатывают системные вызовы гостевых ОС, планировщика задач (уровень S6), диспетчера оборудования (уровень S7) и модуля аппаратной виртуализации (уровень S8). Требования правил политики безопасности, заданные в табличной форме, используются для контроля запросов от гостевых ОС.

Процедура поиска скрытых угроз представляет собой цикл, в котором анализируются списки запросов, на основе значения функции оценки состояния **P**i: если **P**i = true, процесс добавляется в список разрешенных, если **P**i = false, формируется список запрещенных процессов. В результате работы алгоритма создается база данных вредоносного программного обеспечения, которая периодически обновляется. На основе таблиц безопасных операций контролируется активность сетевых приложений и отслеживаются входящие и исходящие пакеты данных.

В четвертой главе производится анализ эффективности предложенных моделей и метода, выполняется этап верификации посредством проведения математического моделирования и экспериментальной проверки разработанного метода и средств противодействия скрытым угрозам информационной безопасности в среде облачных вычислений. Показано, как злоумышленники, используя скрытые для гостевых ОС каналы информационного взаимодействия, способны «обойти» традиционные средства защиты. Только программные средства, созданные на основе декомпозиции иерархических структур и формализации информационных процессов гостевых ОС и подсистем гипервизора, способны выявлять и блокировать подобный класс атак.

Предложена оценка эффективности использования разработанной модели операций для решения задач противодействия скрытым угрозам информационной безопасности в среде облачных вычислений для разных типов гипервизоров. Оценка результатов успешного обнаружения сторонних программных агентов проводилась на тестировочном стенде VIPNet – Coordinator, который объединяет 50 сервисных узлов, 2 сервера, 60 рабочих станций операторов и представляет собой виртуальную защищенную сеть.

На рисунке 4 приведен пример организации программного комплекса верификации команд, генерируемых двумя виртуальными машинами, функционирующих в среде облачных вычислений. Комплекс включает в себя прокси – модуль ядра гостевой ОС и модуль верификации команд. Проксирующий модуль перехватывает обращения к обработчику прерываний и менеджеру памяти, осуществляет контроль операций ввода-вывода при работе с эмуляторами устройств. Модуль верификации контролирует выполнение команд на уровне исполнительного региона процессора.

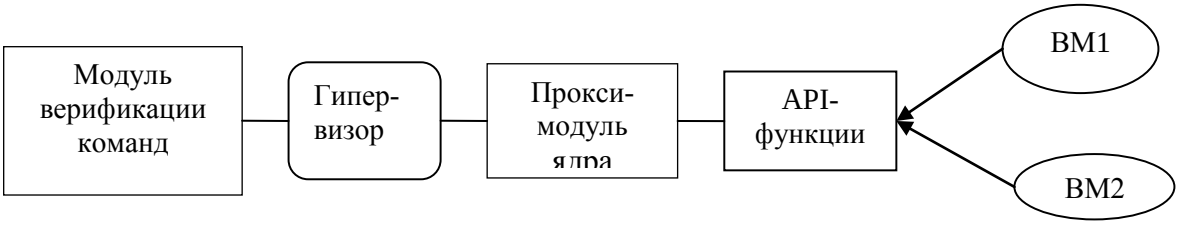

Рисунок 4 Функциональная организация программного комплекса верификации команд

При проведении экспериментальных исследований возможностей модификации гостевых ОС и гипервизора (таблица 3 и таблица 4) использовались различные вредоносные программы: SevenPandora, Hox, HackerDefender, Storm, Croax, Legend, BluePill, VICE Toolkit, DRM, IceBrute, Rustock, Red Dragon.

Таблица 3. Сравнение результатов работы алгоритмов

Программный комплекс защиты	**Количество успешных обнаружений вредоносного ПО**
KasperskyScanner	246
NortonSecurityGuard	1061
VIP NET OfficeFirewall	2479
Monitor - Альфа	2501

Эффективность разработанной системы защиты оценивалось на основе применения разных средств защиты и анализа числа успешных распознаваний и ошибок.

Полученные данные наглядно иллюстрируют, что классические методы контроля и защиты ПО с использованием 4 базовых уровней модели операций S1 – S4 показывают худший результат по сравнению со случаем установки модуля контроля и защиты ПО, функционирующего на уровне S5 при малой интенсивности активных запросов и на уровнях S6 – S7 при пиковой активности. В таблице 4 символом «+» обозначено успешное распознавание угрозы, а символом «–» – ошибка распознавания. Апробация теоретических результатов диссертации и экспериментальная проверка эффективности разработанных моделей, метода защиты и алгоритма предикативной идентификации позволили создать опытный образец программного комплекса «Альфа-монитор» (свидетельство Роспатента № 2014616744 от 03.07.2014 г.), который используется в системах информационной безопасности ряда компаний, в том числе ИнфоТеКС, НПО РУСНЕТ, НПО ФРАКТЕЛ, ОАО РЖД.

Таблица 4.Эффективность обнаружения вредоносного ПО

Название вредоносного ПО и уровни функционирования СЗИ	Hacker Defender, Hox(S1-S3)	Seven Pandora (S3-S5)	Storm (S5)	Croax, Legend (S6)	Ice Brute, Dragon, VICE (S7)	Rustock1, Rustock2, Rustock3, (S7)
KasperskyAntivirus	+	+	–	+	–	–
NortonSecurityCenter	+	+	–	+	+	+
VIP NET OfficeFirewall	+	+	–	+	–	–
Альфа-монитор	+	+	+	+	+	+

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ:

1. Разработана модель скрытых угроз информационной безопасности, учитывающая контекст выполнения операций информационного взаимодействия в среде облачных вычислений.

2. Разработана модель операций, выполняемых над данными при их обработке в среде облачных вычислений, позволяющая формализовать описание информационных процессов в виде мультиграфа транзакций.
3. Разработан метод противодействия скрытым угрозам, основанный на контроле запросов на выделение ресурсов в соответствие с оценкой безопасности выполняемых транзакций.
4. Разработан алгоритм предикативной идентификации угроз, возникающих для подсистем гипервизора при реализации запросов гостевых ОС на выделение информационных ресурсов.
5. Создан опытный образец программного обеспечения «Альфа - монитор» и проведена его успешная апробация в среде облачных вычислений

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

1. **Моляков, А.С. Мультиграфовая модель операций для защиты среды облачных вычислений от скрытых угроз информационной безопасности [Текст] / А.С. Моляков, В.С. Заборовский, А.А. Лукашин // Проблемы информационной безопасности. Компьютерные системы. - СПб.: Изд-во Политех. Ун-та, 2014. – №2. – С. 37 – 40.**
2. **Моляков, А.С. Модель скрытых угроз информационной безопасности в среде облачных вычислений [Текст] / А.С. Моляков, В.С. Заборовский, А.А. Лукашин // Проблемы информационной безопасности. Компьютерные системы. - СПб.: Изд-во Политех. Ун-та, 2014. – №2. – С. 41 – 46**.
3. Моляков, А.С. Исследование новых моделей и методов управления информационной безопасностью с целью противодействия средствам скрытого воздействия [Текст] / А.С. Моляков // Информационная безопасность регионов России (ИБРР-2013). VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2013 г.: материалы конференции / СПОИСУ. – СПб., 2013. –С. 50.
4. **Моляков, А.С.Тихоокеанско-азиатские петафлопсы [Текст] / А.С. Моляков, В. С. Горбунов, П. В. Забеднов // Открытые системы. СУБД. - 2011. –№ 7. – С. 26-29.**
5. **Моляков, А.С. KPROCESSOR_CID_TABLE –факторинг – новый метод в теории компьютерного анализа вирусного кода и программных закладок [Текст] / А.С. Моляков // Проблемы информационной безопасности. Компьютерные системы.- СПб.: Изд-во Политех. Ун-та, 2009. –№1. – С. 7 – 18.**
6. **Моляков, А.С. Метод контроля отображения защищенных сегментов памяти при трансляции виртуальных адресов процессов ОС Windows [Текст]/ А.С. Моляков // Вопросы защиты информации. – М: Изд- во ВИМИ, 2009. - №2. – С. 32-35.**
7. **Моляков, А.С. Новый метод систематического поиска недекларированных возможностей ядра WindowsNT 5. с введением контроляContextHooking и PspCidHooking [Текст] / А.С.Моляков // Журнал Вопросы защиты информации. – М: Изд- во ВИМИ, 2008. - №1. –С. 49 – 55.**
8. **Моляков, А.С. Новые методы поиска скрытых процессов ядра WindowsNT 5.1 [Текст] / А.С. Моляков // Программные продукты и системы.–М.: Изд-во НИИ Центрпрограммсистем,2007.– №4.–С. 43 –45.**

9. **Моляков, А.С. Исследование проектов верхнего и нижнего уровней ПБ ОС Windows [Текст] / А.С. Моляков, А.А. Грушо // Программные продукты и системы.- Тверь: Изд-во НИИ Центрпрограммсистем, 2007.– №4. – С. 45 –47.**

10. **Моляков, А.С. Достоинства и недостатки разных мер защиты информации [Текст]/ А.С. Моляков // Техника и технология. – М.: Изд-во Компания Спутник +, 2007. – №18. – С. 95.**

11. **Моляков, А.С. Исследование скрытых механизмов управления задачами ядра WINDOWS NT5.1 [Текст] /А.С. Моляков // Известия Южного Федерального Университета. Технические науки. – Таганрог: Изд–во ТТИ ЮФУ, 2007. – №1. – С. 139 – 147**

12. Моляков, А.С. Анализ P-полноты языка политики безопасности ОС WINDOWSNT [Текст] / А.С. Моляков // Сборник статей международной научно-технической конференции СIT. – Пенза: Изд-во ПГПУ, 2007. –С. 141 – 148.

13. Моляков, А.С. Использование метода динамического анализа систем автоматизации обнаружения недекларированных возможностей программного обеспечения [Текст] / А.С. Моляков, А.А. Грушо // Материалы 9 Международной научно-практической конференции. – Таганрог: Изд – во ТТИ ЮФУ, 2007. –С. 36 – 38.

14. Моляков, А.С. Исследование ядра WindowsNT 5.1 на платформе Intel3000. Систематический поиск нерегулярных отношений в матрице состояний процессов [Текст] / А.С. Моляков // Материалы 16 Общероссийской научно-технической конференции. – СПб.: Изд-во Политех. Ун-та, 2007. – С.26 – 27.

15. Моляков, А.С. Исследование скрытых механизмов организации ядра WindowsNT5.1 [Текст] / А.С. Моляков // Сборник статей международной научно-технической конференции СIT-2007. - Пенза: Изд-во ПГПУ, 2007. – С. 129 – 134.

16. Моляков, А.С. Исследование неявных механизмов модификации динамического пространства процессов Windows: учебно-методическое пособие [Текст] / А.С. Моляков. – М.: Изд-во Компания Спутник +, 2007. – 67 с.

17. **Моляков, А.С. Наиболее распространенные угрозы безопасности АС [Текст] / А.С. Моляков //Естественные и технические науки. - М.: Изд-во Компания Спутник +, 2006.– №6. –С.254 – 56.**

18. **Моляков, А.С. Обнаружение скрытых каналов в 3 кольце защиты ОС Windows [Текст] / А.С. Моляков // Естественные и технические науки. - М.: Изд-во Компания Спутник +, 2006.– №6. –С.257 – 264**.

19. Моляков,А.С. Исследование ядра WindowsNT 5.1 на целевой платформе Intel 3000: монография [Текст] / А.С. Моляков.–М.: Изд-во Компания Спутник +,2006.– 129 с.

20. Моляков,А.С. Методы поиска скрытых процессов в ОС Windows: учебное пособие [Текст] / А.С. Моляков.– М.: Изд-во Компания Спутник +,2006.–81 с.