На правах рукописи

**МОЛЯКОВ АНДРЕЙ СЕРГЕЕВИЧ**

# МОДЕЛИ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТАЦИОНАРНЫХ И БОРТОВЫХ СУПЕРКОМПЬЮТЕРНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Специальность 2.3.6 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени доктора технических наук

Москва 2023

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Российский государственный гуманитарный университет»

Официальные оппоненты:

**Конявский Валерий Аркадьевич**

доктор технических наук,
ФГАОУ ВО «Московский физико-технический институт», г. Долгопрудный, заведующий кафедрой «Защита информации»

**Лепешкин Олег Михайлович**

доктор технических наук, доцент,
ФГКВОУ ВО «Военная академия связи имени маршала Советского Союза С.М. Буденного», г. Санкт-Петербург, доцент кафедры безопасности инфокоммуникационных систем специального назначения

**Петренко Сергей Анатольевич**

доктор технических наук, профессор,
АНО ВО «Университет Иннополис», г. Иннополис, профессор Центра информационной безопасности

Защита состоится «28» марта 2024 г. в 14:00 часов на заседании диссертационного совета ЮФУ801.02.02 Федерального государственного автономного образовательного учреждения высшего образования «Южный федеральный университет» по адресу: Ростовская обл., г. Таганрог, ул. Шевченко, 2, «Точка кипения» ИТА ЮФУ.

С диссертацией можно ознакомиться в зональной научной библиотеке ЮФУ по адресу: г. Ростов-на-Дону, ул. Зорге, 21-ж и на сайте ФГАОУ ВО «Южный федеральный университет» по адресу: https://hub.sfedu.ru/diss.
Отзывы на автореферат в двух экземплярах, заверенные печатью учреждения, просьба направлять по адресу: 347922, Ростовская обл., г. Таганрог, ГСП-17А, пер. Некрасовский, 44, к. 302, Диссертационный совет ЮФУ801.02.02.

Автореферат разослан «___» января 2024 г.

Ученый секретарь
диссертационного совета ЮФУ801.02.02,
кандидат технических наук, доцент Ельчанинова Н.Б.

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность работы**. В данной работе рассмотрены два типа суперкомпьютеров: *бортовые* (например, «Грифон» или «Комдив») – это компактные высокопроизводительные вычислительные платформы для работы в режиме реального времени и жестких условиях эксплуатации на борту летательных аппаратов, *стационарные* («Ангара» ЕС1740, СТ-2, Tsubame 3.0) – это высокопроизводительные вычислительные платформы для промышленных объектов, центров обработки данных и т.п. Профиль защиты зависит от типа и архитектуры суперкомпьютера (СК). По сравнению со стационарными суперкомпьютерами бортовые супер-ЭВМ обладают ограниченными ресурсами (оперативная память, количество ядер процессора, количество вычислительных блоков), поэтому набор функций безопасности и режимов защиты для них базовый (минимальный).

Для стационарных суперкомпьютеров в зависимости от набора конфигураций заданы три профиля защиты: для малого промышленного кластера уровень защиты средний, для суперкластера крупного технологического объекта – уровень защиты высокий, для масштабных разведывательных или информационно-аналитических центров – уровень защиты максимальный.

В настоящее время в России различными предприятиями ведутся работы по созданию и поставкам вычислительных систем кластерного типа высокой производительности, основу которых составляют коммерчески доступные компоненты и сборочные единицы импортного производства. Подавляющее большинство аппаратных средств, используемых для создания супер-ЭВМ, зарубежного производства, либо сборка конструктивов осуществляется по иностранной лицензии на территории РФ, реализуемая обвязка состоит из недоверенных элементов, импортируемых из-за рубежа.

Высокопроизводительная элементная база вместе с поставляемым системным программным обеспечением (ПО) суперкомпьютеров имеет огромное количество компонентов и представляет собой *недоверенную аппаратуру*, что повышает вероятность применения *средств скрытого информационного воздействия* (ССИВ) и приводит к изменению функциональности, утечке конфиденциальной информации или нарушению работы суперкомпьютеров.

Факты обнаружения вредоносного аппаратного и программного обеспечения в США, России и других странах только подкрепляют эти опасения. При проведении установки, наладки, монтажа, пусконаладочных и иных видов работ, при изменении конфигурации или при обновлении и установке дополнительных программных, технических и программно-технических средств высока угроза внедрения вредоносного ПО локально или по сети. В результате выполнения непреднамеренных или умышленных действий со стороны пользователей, администраторов, обслуживающего технического персонала также высока вероятность выведения из строя либо простоя в функционировании, что недопустимо для современных суперкомпьютеров при выполнении разного класса инженерно-расчетных высоконагруженных задач.

В качестве примера можно привести доклад группы исследователей из компании Positive Technologies, специализирующейся в области информационной безопасности (ИБ), которая в 2017 году обнаружила уязвимость в модуле Intel Management Engine, существующую с 2008 года, которая позволила получить полный доступ к системе и установить вредоносное программно-аппаратное обеспечение, которое не удавалось обнаружить в течение 9 лет.

Актуальность исследования в области создания защищенных национальных суперкомпьютерных платформ подтверждается и «Приоритетными направлениями развития науки, техники и технологий Российской Федерации», утвержденными Указом Президента РФ от 16 декабря 2015 г. № 623.

Следует отметить, что с 2018 года в России действует закон 187-ФЗ «О безопасности критической информационной инфраструктуры», обязывающий организации обеспечить комплексную защиту объектов КИИ, неотъемлемой и важной частью которых являются суперкомпьютеры, специфика которых заключается в следующем: суперкомпьютеры обладают высочайшей производительностью, большим количеством одновременно выполняемых процессов (от сотни тысяч – до миллиона), что определяет трудность отслеживания происходящих в них событий с целью обнаружения вторжений. Высокая параллельность, асинхронность, огромное количество процессов, динамически меняющийся контекст выполняемых операций, сложная сборка инструкций и иерархия выполнения команд, Петабайты данных, которые нужно обрабатывать в режиме реального времени, глобально адресуемая память – все это приводит к тому, что сегменты памяти данных и программ «расплываются» по огромной памяти распределенных процессов, нет точной привязки к доменам защиты, число уровней иерархии обработки запросов не идентифицировано, не соответствует числу уровней защиты, нет интервальных ограничений фильтрации в зависимости от класса и архитектуры СК.

Обрабатываемая с использованием суперкомпьютеров информация обычно связана с решением вопросов национальной безопасности и решением важнейших научно-технических задач, осуществлением управления критически важными инфраструктурами и т.д. Это серьезная мотивация для организации атак.

Пользователи суперкомпьютеров имеют высокую квалификацию и их обычно много, что повышает риски внутренних атак. Высокой квалификацией обладают заинтересованные в атаках на суперкомпьютерные ресурсы злоумышленники, обычно представляющие организованные сообщества, поддерживаемые на государственном уровне. Например, 17 июля 2020 года группа реагирования на инциденты информационной безопасности (CSIRT) опубликовала отчет, в котором говорилось, что под ударом тщательно спланированных компьютерных атак оказались Стэнфордский национальный центр атмосферных исследований, Суперкомпьютерный центр в Сан-Диего и Национальный центр суперкомпьютерных приложений при Иллинойсском университете, Суперкомпьютерный центр в Лос-Аламос и др. В России также наблюдается взрывной рост кибератак на суперкомпьютерные центры Яндекса и Сбербанка, кардинальное увеличение их мощности и использование новых тактик со стороны злоумышленников.

Более того, существующие и успешно внедрённые программно-технические решения промышленного комплекса России ориентированы на традиционные вычислительные кластеры и не учитывают специфики суперкомпьютеров, о которой говорилось ранее. В качестве примера можно привести реализацию средств защиты информации Ростатома, в основе которой лежат только базовые программно-технические компоненты на базе Scientific Linux для платформы x86_64. При этом не учитываются особенности работы процессоров и контроллеров с разными уровнями иерархии команд. Однако, как показали результаты проведенных научно-исследовательских и опытно-конструкторских работ китайских специалистов из Национального суперкомпьютерного центра Чанг-Ша и японских специалистов из Национального суперкомпьютерного центра Осаки, без интеграции с аппаратной транзакционной памятью и введения многоуровневого контроля невозможно создать доверенную среду с использованием широко распространенных коммерческих программно-аппаратных средств и решить задачу обнаружения и идентификации разного типа угроз на всех уровнях иерархии выполнения запросов СК.

Следует отметить, что для создания подсистемы обеспечения безопасности серверов и рабочих станций разработчики обычно используют: *проактивные методы*, основной целью которых является предотвращение заражения системы, и *реактивные методы,* суть которых заключается в сигнатурном поиске уже известного вредоносного ПО. Переходя на уровень инженерных решений для суперкомпьютерных платформ, производители оборудования реализовали для системных разработчиков встроенную полнофункциональную поддержку технологии виртуализации для разного набора микропроцессоров и микроконтроллеров.

Других базовых (штатных) функций безопасности у аппаратных модулей и сборочных конструктивов, из которых собираются компоненты СК, просто нет. С использованием технологии виртуализации можно реализовать принципы *кибериммунитета*, основанные на разбиении системы на изолированные домены безопасности, многоуровневом контроле всех взаимодействий между доменами безопасности, обеспечении гарантированной защищенности вычислительной среды. Для каждого взаимодействия доменов безопасности монитор обращений возвращает решение (булево значение) в виде функции оценки безопасности состояний СК, соответствует ли это взаимодействие политике безопасности.

Из всего выше сказанного можно сделать вывод о том, что в современных условиях средства защиты информации (СЗИ) суперкомпьютеров разрабатываются с использованием виртуализации оборудования, поскольку она позволяет повысить гибкость использования и функционирования оборудования, обеспечивая этим совместное функционирование разных операционных систем, поддержку технического парка ЭВМ с разной архитектурой сборки, оптимизировать развиваемую производительность и энергоэффективность, обеспечить реконфигурируемость не только для восстановления после сбоев и отказов аппаратных средств, но и после компьютерных атак. Перечисленные особенности определяют научную проблему создания новой методологии обнаружения компьютерных атак на СК. Основу подхода составляют метод реактивной защиты и метод реконфигурации среды проактивной защиты, позволяющие обнаруживать любые типы компьютерных атак на всех уровнях иерархии выполнения запросов и противодействовать им путем автоматической реконфигурации структуры конфигурации исполняемой среды СК на недоверенной аппаратуре.

**Степень разработанности темы исследования.** Известно значительное число работ, посвященных созданию защищенных информационных систем. Например, в работах В.А. Курбатова, П.Д. Зегжды, А.А. Гладких разработаны и проиллюстрированы методы и подходы, предназначенные для защиты только отдельных серверов виртуализации в составе производительных кластеров. В теоретических и практических исследованиях, проведенных А.А. Грушо, В.С. Заборовским, С. Воглом, Р. Сэйлером, Ф. Мортинелли, Дж. Рутковской, предложены и разработаны принципы и методы в области обеспечения защиты на основе мандатных и ролевых политик безопасности, методы обнаружения средств скрытого информационного воздействия для киберфизических систем, построенных на базе рабочих станций и серверов предыдущего поколения, без учета специфики современных суперкомпьютеров. Работы О.В. Казарина и В.Ю. Скибы посвящены созданию методов и средств проактивной защиты программного обеспечения, однако авторам так и не удалось решить проблему реализации доверенной среды выполнения программ на недоверенном оборудовании для суперкомпьютерных систем. Таким образом, можно сделать вывод о том, что тема создания средств обеспечения информационной безопасности суперкомпьютерных вычислительных систем на основе разработки моделей и методов гибридной защиты за счет использования средств виртуализации (гипервизоров), является актуальной, новой и пока нерешенной, исходя из анализа работ зарубежных и российских специалистов.

При работе на недоверенной аппаратуре для создания доверенной программной среды предложено использовать компонент – верификатор команд процессора, а интегрированная защита суперкомпьютеров реализована в виде многомодульного мультидоменного гипервизора в связке с контроллерами транзакционной памяти.

**Факторы доверительности и допущения**, делающие недоверенную среду функционирования защищенной, следующие:

1) Объем кода гипервизора невелик по сравнению с ОС и приложениями, поэтому в нем проще обеспечить отсутствие уязвимостей. Все действия и события внутри виртуализованной системы обратимы – атаки могут быть оперативно нейтрализованы путем отката или сброса в исходное состояние.

2) Контроль обмена виртуализованной системы с внешней средой со стороны гипервизора позволяет отказаться от досконального исследования самих сред исполнения.

3) Аппаратная транзакционная память гарантирует атомарность и изолированность параллельно выполняемых задач, а также привязывает сегменты данных и программ к определенному домену защиты. Также поддерживается мультидоменный режим (набор разных доменов защиты с учетом уровней привилегий).

4) Мониторинг событий на всех уровнях иерархии выполнения запросов СК. Все операции транслируются гипервизором и контролируются верификатором команд. Параллельные процессы не могут «расплываться» по всем участкам памяти. Операции выполняются в определенном режиме работы процессора и обращаются только к выделенным им сегментам памяти данных и программ, а не случайно перемещаются по всей оперативной памяти.

5) Функционирование модуля верификации реализовано на более привилегированном уровне, чем ядро управляющей ОС и монитор виртуальных машин, благодаря чему осуществляется работа гипервизора напрямую с контроллерами транзакционной памяти и процессорами.

6) Взаимодействие процессов пользователя происходит с компонентами гипервизора, который создает изолированную среду исполнения. Компоненты гипервизора контролируют обращения к объектам файловой системы и стекам сетевых протоколов, осуществляют контроль последовательности выполнения запросов на выделение вычислительных ресурсов на всех уровнях иерархии. Изолированность (изолированная программная среда) гарантирует то, что параллельно выполняемые задачи не влияют на результат транзакции, обеспечивается надежная изоляция адресного пространства разных пользователей.

7) Выдаваемые запросы изначально связываются с некоторой информационной структурой, называемой тегом. При прохождении запросом уровня защиты он не выполняется, а только происходит планирование действий для него на этом уровне и фиксация информации о контексте их выполнения, производится соответствующее этому изменение тега запроса и задаются интервально-временные ограничения выполнения команд.

8) По мере продвижения запроса через уровни в теге накапливается информация в виде его межуровневой трассы. Работа с тегами запросов на разных уровнях защиты производится модулями гипервизора. Атрибуты доступа к объекту и привилегии субъекта, связи между ними формализуются в виде набора (конъюнкции) предикатов. Отслеживать взаимодействие и контролировать доступ можно по набору характерных признаков – маркеров, представленных в виде кортежей логических переменных.

9) При изменении значений переменных и интервально-временных ограничений в указанной логической иерархической структуре, меняются идентификация вершин трассы и нумерация маршрута прохождения, что свидетельствует о подозрительной активности в системе.

10) Требования политики безопасности формулируются в терминах, которые задают последовательность обработки операций и ограничений на возможность повышения привилегий процессов. Ограничение на повышение привилегий и контроль контекста операций задаются значениями функции оценки безопасности.

**Объект исследования**: системы защиты суперкомпьютерных вычислительных систем в стационарном и бортовом исполнении.

**Предмет исследования**: модели, методы и алгоритмы обеспечения информационной безопасности суперкомпьютерных вычислительных систем с применением средств виртуализации.

**Цели и задачи диссертационной работы.**

**Цель диссертационной работы:** получение и поддержание максимального уровня гарантированной защищенности суперкомпьютеров на основе разработки моделей и методов гибридной (реактивной и проактивной) защиты за счет использования

гипервизоров, обеспечивающих надёжную защиту от угроз информационной безопасности, реализуемых с использованием средств скрытого информационного воздействия.

В соответствии с этим были поставлены и решены следующие **основные задачи работы:**

1) Разработка теоретических и научно-методических принципов защиты суперкомпьютеров с использованием средств виртуализации.

2) Разработка модели угроз целостности среды выполнения процессов с учетом специфики суперкомпьютеров.

3) Разработка модели безопасных операций, которая учитывает новый тип угроз, связанных с неоднозначностью состояний выполнения прикладных и системных программ при работе в недоверенной среде суперкомпьютеров.

4) Разработка и исследование метода реактивной защиты суперкомпьютеров, заключающегося в виртуализации среды выполнения процессов на недоверенном оборудовании.

5) Разработка и исследование метода реконфигурации среды выполнения программ проактивной защиты суперкомпьютеров с учетом требований мобильности (встроенности производимых вычислений) и факторов доверительности.

6) Разработка методики тестирования уровня защищенности суперкомпьютеров, основанной на алгоритме “маркерного” сканирования.

7) Разработка программно-технических решений, обеспечивающих гарантированную защиту от угроз информационной безопасности, реализуемых с использованием средств скрытого информационного воздействия.

**Методы исследования**. Для решения поставленных задач в диссертационной работе использовались методы дискретной и вычислительной математики, теории графов, теории вероятностей, теории защиты информации, методы математического и численного моделирования, системный анализ, статистические методы (в частности корреляционный анализ), научный аппарат, основанный на принципах и положениях темпоральной логики.

**Достоверность полученных результатов** обусловлена корректным применением методов исследований и подтверждается результатами практического использования, а также соответствующими актами внедрения (реализации), схемами и чертежами рабочей конструкторской документации, их внутренней непротиворечивостью и адекватностью физическим представлениям об исследуемом процессе. Предложенные в диссертационной работе результаты теоретически обоснованы и не противоречат известным и достоверно подтверждённым результатам исследований других авторов.

**Научная проблема**: для инженерии и отрасли промышленности на примере создания защищенных суперкомпьютерных систем известна как *проблема супервентности*: с учетом высокой асинхронности и многосвязности процессов, огромного объема обрабатываемых данных нет логического соответствия между изменениями программ среды исполнения СК и изменениями компонентов аппаратуры с точки зрения реализации изолированной среды и контроля правил политик безопасности (ПБ). Следовательно, для создания доверенной среды выполнения программ суперкомпьютеров на недоверенном оборудовании, обеспечивающей надёжную защиту от угроз информационной безопасности, реализуемых с использованием ССИВ, необходимо разработать и внедрить механизмы многоуровневого контроля: любые преобразования, трансляции операций гипервизором при взаимодействии с аппаратурой должны быть безопасными, с точки зрения реализации механизмов идентификации и верификации.

**Научная новизна**. В диссертации получены следующие новые научные результаты:

1) Разработаны теоретические и научно-методические принципы защиты суперкомпьютеров с использованием средств виртуализации, *основанные* на построении и формализации универсальных и равномерных функций оценки безопасных состояний СК для заданных классов операций, *отличающиеся* нахождением в n-мерной алгебраической системе инварианта, *позволяющие* решить научную проблему супервентности для отрасли

промышленности. Судя по открытым международным и отечественным источникам, исследования суперкомпьютеров в качестве объектов защиты проводятся впервые.

2) Разработана модель угроз целостности среды выполнения процессов, *основанная* на новой парадигме написания правил политики безопасности, *отличающаяся* заданием сущностей вместо классической связки «субъект, объект, предикат» – «субъект», «объект» и «дескриптор оценки безопасности состояний», *позволяющая* описать и формализовать каждую i-ую угрозу аргументов в виде конъюнкции предикатов из восьми логических переменных.

3) Разработана модель безопасных операций, *основанная* на декомпозиции информационных процессов в виде 8-уровневой иерархической структуры и принципах кибериммунитета, *отличающаяся* оценкой безопасности состояний в виде логической функции и проверки истинности принимаемых решений на каждой возможной интерпретации с учетом специфики суперкомпьютеров в виде временной и пространственной сложности, *позволяющая* идентифицировать и блокировать разные классы уязвимостей на всех уровнях иерархии выполнения запросов, что подтверждается сформулированным условием разрешимости и доказанной теоремой.

4) Разработан и исследован метод реактивной защиты суперкомпьютеров, *основанный* на виртуализации среды выполнения процессов, если вычисленный дескриптор состояния попадает в зону «риска», *отличающийся* применением траекторий вычислений дескрипторов оценки безопасности состояний на структурах Крипке, *позволяющий* создать единую технологию выявления уязвимостей и реализовать полный контроль контекста и тайминга выполняемых операций на недоверенной аппаратуре.

5) Разработан и исследован метод реконфигурации среды выполнения проактивной защиты суперкомпьютеров, *основанный* на парадигме темпоральной логики для проверки истинности принимаемых решений на структурах Крипке, *отличающийся* вычислением доверительной вероятности в качестве показателя защищенности компонентов среды на наборах тегированных данных в виде согласованной вариации факторных и результативных признаков, *позволяющий* на ранней стадии обнаруживать новые классы уязвимостей и противодействовать им путем автоматической реконфигурации структуры.

6) Разработана методика тестирования уровня защищенности, *основанная* на алгоритме “маркерного” сканирования, *отличающаяся* использованием набора меток: сочетаниям меток сопоставляются признаки скрытых угроз и действия, отвечающие требованиям выбранной политики информационной безопасности, *позволяющая* повысить уровень защищенности вычислительных ресурсов СК и минимизировать ошибки 1-го и 2-го рода.

7) Разработаны программно-технические решения, *основанные* на разработанных моделях и методах, *отличающиеся* минимальными затратами ресурсов для создания обучающих кластерных зон и на обучение по сравнению с существующими технологическими решениями на основе скрытых марковских моделей (с использованием алгоритма Баумана-Уэлча), *позволяющие* реализовать гарантированно защищенные системы, адаптированные к потоку входных данных и наборам конфигураций вычислительной среды.

**Теоретическая значимость** состоит в том, что разработанные и предложенные модели и методы, составляющие основу реактивной и проактивной защиты, развивают ряд положений теории информационной безопасности, базирующихся на формализации информационных процессов суперкомпьютеров в виде «вычисляемой свертки состояний среды выполнения», введены новые теоретические и научно-методические принципы для создания защищенных СК. Доказана теорема о равномерной перечислимости функций СК. Сформулировано условие разрешимости проблемы установки логического соответствия (супервентности) между изменениями программ среды исполнения СК и изменениями компонентов аппаратуры: если число уровней иерархии равно восьми, то процессы наблюдаемы на всех интерфейсных уровнях, любые трансляции операций гипервизором

становятся безопасными. Правила политики безопасности задаются в виде модальных структур темпоральной логики CTL, учитывающих контекст выполнения и тайминг операций (запросов). В качестве спецификации системы используется структура Крипке. Введено новое понятие «дескриптор оценки безопасности состояний системы». Введена новая характеристика для создания защищенных суперпроизводительных систем: коэффициент готовности к безопасной эксплуатации СК.

**Практическая ценность** заключается в разработке технологии и программно-технических средств на основе предложенных моделей и методов, составляющих принципы реактивной и проактивной защиты. С учетом специфики суперкомпьютеров предложено принципиально *новое технологическое решение*, создающее изолированную среду исполнения программ в виде 8-уровневой «песочницы» с реализацией контролирующих механизмов как на уровне гипервизоров, так и на уровне контроллеров транзакционной памяти. Технология следящих действий со стороны гипервизоров и управляющих ОС суперкомпьютеров, основанная на использовании проксирующих модулей и верификатора команд, позволяет по сравнению с существующими отечественными и зарубежными подходами значительно повысить уровень защищенности СК. Таким образом, решена важная научно-техническая проблема в области создания средств защиты информации для нового класса систем – стационарных и бортовых СК. Все существовавшие на сегодняшний день СЗИ являлись программно-техническими компонентами самой защищаемой системы, без интеграции с аппаратной транзакционной памятью и введения многоуровневого контроля невозможно было решить задачу обнаружения и идентификации разного типа угроз на всех уровнях иерархии выполнения запросов СК. В ходе экспериментальных исследований получены *новые научные результаты*, подтверждающие эффективность и минимальную потерю производительности применения технологии аппаратной виртуализации в виде многоуровневой «песочницы» для перспективных СК по сравнению с использованием традиционных кластеров. Предложенные технологические решения в нескольких вариантах позволяют снизить затраты на производство за счёт переноса большей части испытаний с опытных образцов на программное обеспечение.

**Результаты, выносимые на защиту**:

1) Теоретические и научно-методические принципы защиты стационарных и бортовых суперкомпьютеров с использованием средств виртуализации.
2) Модель безопасных операций, основанная на декомпозиции информационных процессов в виде 8-уровневой иерархической структуры и принципах кибериммунитета.
3) Модель угроз целостности среды выполнения процессов, основанная на новой парадигме написания правил политики безопасности.
4) Метод реактивной защиты суперкомпьютеров, основанный на виртуализации среды выполнения процессов, если вычисленный дескриптор состояния попадает в зону «риска».
5) Метод реконфигурации среды выполнения проактивной защиты суперкомпьютеров, основанный на парадигме темпоральной логики для проверки истинности принимаемых решений на структурах Крипке.
6) Программно-технические решения, основанные на разработанных моделях и методах.

**Внедрение научных результатов** подтверждается наличием актов о внедрении (реализации) и структурными схемами (чертежами). Результаты теоретических и экспериментальных исследований, полученные в ходе выполнения диссертационной работы, были успешно внедрены автором при разработке программно-технического комплекса «Альфа-монитор» для российских суперкомпьютерных платформ «Ангара» серии ЕС1740, в рамках российского проекта по созданию высокопроизводительных мобильных (бортовых) вычислительных средств морского, наземного и воздушного базирования, при выполнении научно-исследовательской работы Минобрнауки РФ «Разработка методов построения защищенных облачных высокопроизводительных

виртуальных вычислительных инфраструктур гетерогенной архитектуры для решения экстремальных задач в фундаментальных, научных, образовательных и производственных сферах» (регистрационный номер 88062011); авторские изобретательские и рационализаторские предложения реализованы в рамках китайского проекта по разработке защищенных суперкомпьютерных вычислительных комплексов серии Tian-he/CT-2 (ОКР шифр «Удар грома»), в рамках японского проекта по созданию суперкомпьютера с высокими показателями производительности и защищенности серии Tsubame 3.0 (ОКР шифр «Стрела времени»), а также в учебном процессе и научных исследованиях на кафедре «Комплексная защита информации» ФГБОУ ВО «РГГУ» по дисциплинам «Программно-аппаратные средства защиты информации. Основная часть», «Актуальные тенденции в области защиты информации», «Безопасность операционных систем».

**Апробация результатов работы**. Основные результаты работы были представлены и обсуждены на следующих конференциях и семинарах: Научно-практическая конференция MicroSoft «Современные подходы в построении защищенных систем», Москва, 2011 г.; Общероссийская научно-техническая конференция «Информационная безопасность регионов России», Санкт-Петербург, 2013 г.; 9-я Всероссийская конференция ITSF, Казань 2015 г.; научный семинар «Проблемы современных информационно-вычислительных систем», Москва, 2014 г.; Московский суперкомпьютерный форум, Москва, 2017 г.; Всероссийская научно-практическая конференция «Современные аспекты развития науки, образования и модернизации промышленности», Таганрог, 2016 г; VII международная научно-практическая конференция «Управление информационной безопасностью в современном обществе», Москва, 2019 г.; Международная конференция «World Conference on Smart Trends in Systems, Security and Sustainability (WS4 2019)», Лондон, 2019 г.; Международная научно-практическая конференция «Информационная безопасность: вчера, сегодня, завтра», Москва, 2019 г.; ежегодный научный семинар в СПИИ РАН, Санкт-Петербург, 2019 г.; научный семинар в ФГБУ «3ЦНИИ» Минобороны России, Москва, 2020 г.; Международная научно-практическая конференция по компьютерной и информационной безопасности (INFSEC 2021), Екатеринбург, 2021 г.; Международная научно-практическая конференция ICICT 2022, London, 2023.

**Публикации**. Основные результаты по теме диссертации опубликованы в 31 научной печатной работе, из которых 10 – в ведущих рецензируемых научных изданиях, входящих в перечень ВАК РФ; 6 – в международных изданиях, индексируемых Scopus; 15 – в материалах конференций и других научных изданиях. Также автором получено 2 патента РФ на изобретения и 1 свидетельство о государственной регистрации программы для ЭВМ.

**Соответствие паспорту специальности**. Проведенное исследование и полученные в его ходе результаты соответствуют п. 3 «Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса» (в части разработки моделей, методов и средств идентификации угроз информационной безопасности суперкомпьютеров) и п. 15 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» (на примере создания новых принципов и инновационных технологических решений для подсистемы обеспечения безопасности российских и зарубежных суперкомпьютерных платформ на базе модулей «Альфа-монитор») определения специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» паспорта специальностей ВАК (технические науки).

**Личный вклад автора**. Все результаты, представленные в диссертационной работе, получены лично автором в процессе выполнения научно-исследовательских и опытно-конструкторских работ. На основе аксиоматической теории разработана и предложена новая парадигма написания правил политики безопасности, отличающаяся заданием новых сущностей вместо классической связки «субъект, объект, предикат» – «субъект», «объект» и «дескриптор оценки безопасности состояний». В работе решена важная научная проблема

супервентности для отрасли промышленности, связанной с проектированием и внедрением средств защиты информации для суперкомпьютеров в стационарном и бортовом исполнении. Личный вклад автора в теорию (с точки зрения математических подходов и теории информационной безопасности):

1) Сформулировано условие разрешимости задачи идентификации на всех уровнях иерархии команд и доказана теорема.

2) Формализация каждой i-ой угрозы аргументов в виде конъюнкции предикатов из восьми логических переменных.

3) Спецификация на структурах Крипке с использованием темпоральной логики CTL.

4) Вычисление доверительной вероятности в качестве показателя защищенности компонентов среды.

**Структура и объем диссертационного исследования**. Диссертация состоит из введения, пяти глав, заключения и 4 приложений. Основной материал изложен на 280 страницах. Полный объем диссертации составляет 309 страниц с 40 рисунками и 22 таблицами. Список литературы содержит 128 наименований.

## СОДЕРЖАНИЕ ДИССЕРТАЦИИ

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

**В первой главе** представлен обзор основных методов и проблем в области обеспечения информационной безопасности стационарных и бортовых СК, приведен анализ существующих технологий в области создания защищенных СК. Главная проблема заключается в том, что нет доверия к работе сложных систем, так как отсутствуют средства контроля выполнения операций на всех этапах их «порождений». Некоторые запросы в определенный момент времени могут нарушать требования политик безопасности, формируя «ложные транзакции». Более того, в современных суперкомпьютерных системах объем обрабатываемых данных составляет Пбайты ($10^{15}$ вычислений операций с плавающей точкой в секунду). В результате проведенного анализа отмечено, что суперкомпьютерные вычислительные системы стали играть центральную роль в современной науке и технике, чего раньше никогда не было. Основываясь на определениях *функциональная безопасность* (ГОСТ 61508, ГОСТ 62061), *информационная безопасность* (ГОСТ 27000), *кибербезопасность* (ГОСТ 62443), *кибериммунитет* (ГОСТ МЭК 62443 4-1:2018), информационная безопасность стационарных и бортовых суперкомпьютерных вычислительных систем дополнена новым понятием «дескриптор оценки безопасности состояний системы».

*Дескриптор оценки безопасности состояний системы* – это свертка состояний среды исполнения (аппаратной или виртуальной) и системного программного обеспечения» с учетом механизмов самоконфигурации и самоконтроля, которая вычисляется на основе атрибутов протекающих процессов, которые реализуются на уровне ядер микропроцессоров и среды межсетевого взаимодействия. У всех процессов вычисляются дескрипторы и задаются методы их обработки – get, set, delete и т.п.

В конце главы формулируется вывод о необходимости разработки новой модели обеспечения ИБ суперкомпьютеров с поддержкой виртуализации и с элементами принципиально новой архитектуры. На основе проведённого анализа и оценки влияния новых угроз на состояние защищённости ресурсов суперкомпьютерных комплексов в главе определена цель диссертационного исследования и сформулирован перечень научно-технических задач, решение которых обеспечивает ее достижение.

**Во второй главе** введены новые теоретические и научно-методические принципы защиты суперкомпьютеров с использованием средств виртуализации, решена проблема супервентности. Доказана теорема о равномерной перечислимости функций СК. При этом стационарные и бортовые суперкомпьютеры рассматриваются как объект исследований впервые. Сформулировано условие разрешимости проблемы установки логического соответствия (супервентности) между изменениями программ среды исполнения СК и изменениями компонентов аппаратуры: если число уровней иерархии равно восьми, то процессы наблюдаемы на всех интерфейсных уровнях, любые трансляции операций гипервизором становятся безопасными.

*Теорема1*. Класс A операций на кольце вычетов по модулю m *равномерно перечислимым,* а функция вычисления хеш-значений F – *универсальной* функция класса A только в том случае, если число уровней иерархии (вложенности) равно восьми.

*Доказательство*. Фактически, операции выполняются над кортежами данных, представляющими собой набор i-ых элементов алгебраической структуры (бит, атомарный предикат, конъюнкцию предиката, любой набор предикативных и функциональных символов, вектор-переменная, скаляр, вещественное число) любой размерности m (независимо от кодировок и позиционной системы счисления). Мы работаем с матрицами, где количество строк равно числу вложенности пространства вычислений N, а i-ый столбец – элемент структуры размерностью m в кольце вычетов Z(m).

С учетом расчетной формулы (4) каждый сомножитель представляет собой геометрическую убывающую прогрессию. Нам нужно, чтобы значение представляло периодическую дробь любого значения n, с точностью до n-го знака после запятой никаких новых эффектов не было. Более того, выражение должно быть равно нулю (*условие1* – максимально приближенное значение к нулю), каждый i-ый элемент произведения должен приближаться к нулю, но при этом надо, чтобы выполнялось и условие равномерности вычислений. С изменением разрядности n, когда выполняются операции, отображение должно быть инвариантным (*условие 2*).

Рассмотрим ряд натуральных чисел, задающих набор возможного числа уровней иерархии: {1, 2 … , 9}.

1 – нейтральный элемент. Начнем вычисления с 2 и закончим 9:

N = 2, Q = 0,33333 = 0,(3);
N = 3, Q = 0,25;
N = 4, Q = 0,2;
N = 5, Q = 0,1666666 = 0,1(6);
N = 6, Q = 0,142857;
N = 7, Q = 0,125;
N = 8, Q = 0,111111 = 0,(1);
N = 9, Q = 0,1.

Наиболее подходящие значения: 0,1 и 0,(1). Двум условиям удовлетворяет только решение N = 8. Что и требовалось доказать. Более того, в диссертации предложена эффективная нумерация класса A, поскольку с изменением размерности параметра n не меняются регулярные отношения между элементами множества, не появляются новые свойства у объектов нашей алгебраической структуры.

*Главный результат теоретических выкладок* состоит в том, что мы доказали универсальность и равномерность для заданных классов операций функциональных преобразований. Независимо от архитектуры вычислительных узлов СК найдено такое число уровней иерархии (N = 8), что в алгебраической системе существует инвариант. Если оценивать временные параметры, данное свойство регулярности сохраняется неопределенно долго (от 0 до + ∞). Классическая логика высказываний – это “черно-белая” модель, высказывания статичны, неизменны во времени. В обычной логике высказываний адекватно не формализуются предложения, в которых явно или не явно присутствуют свойства, истинность которых изменяется со временем.

Предложенный подход к описанию операций основан на классификации рисков нарушения информационной безопасности и анализе контекста выполнения исходящих директив, посредством которых могут передаваться данные в обход требований принятой политики безопасности, что приводит к нарушению защищенности ресурсов вычислительных узлов. Обычно 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 j становится возможным только при выполнении условия $O_m[t] = O_m[t_0]$, где Subj – субъект доступа, $O_m$ – объект доступа, j, m – номера объектов. Однако для СК признак неизменности не может быть константой неопределенно долго: запускается одновременно огромное количество процессов. Для описания состояний субъектов и объектов доступа нужна темпоральная логика.

*Темпоральная логика CTL (Логика дерева вычислений)* – это логика времени ветвления, что означает, что ее модель времени представляет собой древовидную структуру, в которой будущее не определено, но в будущем есть разные пути. Темпоральные логики ветвящегося времени рассматривают возможные вычисления (пути на дереве) – траектории на развертке структуры Крипке. Каждое состояние может иметь не одну, а множество цепочек – продолжений, и является корнем своего дерева историй (вычислений).

Формально вычисление структуры Крипке можно представить как отображение натурального ряда в множество состояний структуры. Правила политик безопасности задаются в виде модальных конструкций в терминах темпоральной логики. Значение уровня привилегий представляет ряд десятичных чисел от 0 до 7. Все процессы распределены по доменам в соответствии с уровнем привилегий. Если происходят изменения в структуре выполнения процессов, то изменение уровня привилегий индексируется на единицу, при этом можно мигрировать только между соседними доменами.

Кодирование признаков идентификации – набор или конъюнкция простых предикатов, на которых задана формула Fi. Наборы конфигураций, адаптированных к разным контекстам выполнения операций, в виде матриц правил доступа сохраняются агентами гипервизора в памяти контроллера транзакционной памяти. В процессе обучения обновляются и корректируются правила политики безопасности. Система динамически эволюционирует и модифицирует наборы модальных правил на основе грамматик темпоральной логики CTL по реагированию на сигнальные события.

**В третьей главе** с целью повышения уровня безопасности и защищенности суперкомпьютеров предложены и разработаны модель угроз целостности среды выполнения процессов СК, модель безопасных операций, введена функция оценки безопасности состояний, осуществляющая контроль контекста выполняемых операций. Для каждого заказчика можно создать готовый набор шаблонов виртуальной среды с набором нужного предустановленного ПО под контролем защищенного гипервизора. Экономятся расходы на дополнительных средствах создания доверенной среды и учитываются все функциональные требования еще на этапе разработки и внедрения системы.

Работа технологически осуществляется в многоуровневой «песочнице», что позволяет создавать моделирующие расчетные стенды для промышленного внедрения всей линейки существующих вычислительных средств и поддерживать различные кластерные системы, мейнфреймы, обычные персональные компьютеры и бортовые супер-ЭВМ, суперкомпьютеры нового поколения для внедрения разработанных решений.

Предложено использовать *модель угроз целостности среды* выполнения процессов СК, в которой вместо классической связки «субъект, объект, предикат» реализована новая парадигма написания правил политики безопасности и заданы новые сущности – «субъект», «объект» и «дескриптор оценки безопасности состояний»: для каждой i-ой угрозы вычисляется значение функции оценки безопасности состояний, аргументы которой заданы в виде конъюнкции предикатов из восьми логических переменных, субъектами являются гостевые и управляющие ОС (порождаемые ими запросы), а объектами – компоненты гипервизора и контроллера транзакционной памяти.

Требования политики безопасности формулируются в терминах, которые задают последовательность обработки операций и ограничений на возможность повышения привилегий процессов. При этом на каждом уровне модели операций ведется протоколирование событий и результатов, включая такие параметры, как Time – время и Result – результат выполнения операций.

Ограничение на повышение привилегий и контроль переходов при изменении контекста операций задаются значениями функции оценки безопасности состояний Fi, аргументы которой заданы в виде конъюнкции предикатов из восьми логических переменных, а контроль выполнения процессов, порождаемых субъектами доступа, реализуется на основе принципа наименьших привилегий.

Модель угроз целостности среды выполнения программ для высокопроизводительных комплексов и автоматизированных систем, использующих элементы суперкомпьютерных технологий, в части описания «субъект защиты-объект защиты» формализована в виде кортежа:

< Source, Services, Devices, {proc}, Actions,{hv},{vm}, SecurityRoles > (1),

где Source – авторизованные субъекты доступа; Source = $S^H \cup S^O$, где $S^H$ – множество субъектов гипервизора, а $S^O$ – множество субъектов гостевой и хостовой ОС; Services – шаблоны политик безопасности; Devices – аппаратные устройства, управляемые гипервизором и контроллером транзакционной памяти; {proc} – множество субъектов вредоносного воздействия; Actions – операции субъекта; {hv} – множество компонент гипервизора и контроллера транзакционной памяти; {vm} – объекты воздействия; Security-Roles – механизмы противодействия (идентификации состояний в зависимости от набора кортежа логических переменных функции Fi).

Для формализации описания рассматриваемых процессов автором предложена *модель безопасных операций*, учитывающая все режимы функционирования процессорных устройств. Сравнение авторской модели угроз с существующими классическими моделями представлено в таблице 1. Видно, что все существующие на сегодняшний день наиболее распространенные модели угроз не учитывают специфики суперкомпьютеров разного класса, ориентированы только на традиционные кластеры и информационные системы.

Термин «маркер» означает набор определенных признаков, представленных в виде кортежа логических переменных. Вместо классического сигнатурного распознавания используются генеративные таблицы гипервизора. Признак допустимости операций задается в виде логической функции (2).

Главные компоненты любого суперкомпьютера – вычислительные узлы с многоядерными процессорами, многосокетными материнскими платами, памятью, внутриузловой коммуникационной сетью и сетевыми интерфейсами, а также межузловая коммуникационная сеть. Все операции по работе с локальной или глобально-адресуемой распределенной памятью осуществляются контроллером аппаратной транзакционной памяти.

**Таблица 1 – Сравнение моделей угроз**

| **Название модели** | **Уровни угроз безопасности** | **Оценка уровня защищенности** | **Объект защиты** |
|---|---|---|---|
| Модель угроз NIST & MITRE (вербальная модель с элементами статистической обработки и визуализации выходных данных) | Критичный<br>Высокий<br>Средний<br>Низкий | Балльные оценки экспертов или шкала таблицы показателей | Рабочие станции, мобильные устройства, виртуальная инфраструктура, серверы коммуникационной среды, СУБД, ERP-системы |
| Модель угроз CyberCop & CERT (вербальная модель с элементами прогнозирования на основе экстраполяции данных) | Критичный<br>Высокий<br>Средний<br>Низкий | Балльные оценки экспертов или шкала таблицы показателей | Рабочие станции, мобильные устройства, виртуальная инфраструктура, серверы коммуникационной среды, СУБД, ERP-системы |
| Модель угроз ФСТЭК (вербальная модель с элементами моделирования угроз) | Высокий<br>Базовый повышенный<br>Базовый<br>Низкий | Балльные оценки экспертов или шкала таблицы показателей | Рабочие станции, информационно-телекоммуникационные системы, государственные информационные системы |
| Модель угроз Росатома (вербальная модель с элементами моделирования угроз) | Критичный<br>Высокий<br>Средний<br>Низкий | Балльные оценки экспертов или шкала таблицы показателей | Рабочие станции, мейнфреймы |
| Авторская модель угроз (формализованная модель) | Максимальный<br>Высокий<br>Средний<br>Базовый повышенный<br>Базовый<br>Низкий | Использование функции оценки безопасности состояний компонентов СК Fi | Промышленные кластеры, средние суперкластеры, суперкомпьютеры стратегического класса, бортовые Супер-ЭВМ |

Процессорные модули могут функционировать в разных режимах. Для учета всех режимов функционирования многоядерных процессорных устройств в разработанной модели операций введено четыре кольца защиты, а именно: Priv0 – уровень привилегий команд процессора (IPL_LEVEL), Priv1 – уровень привилегий ядра ОС (KERNEL_LEVEL), Priv2 – уровень привилегий администратора безопасности (SUPERVISOR_LEVEL), Priv3 – уровень привилегий пользователей (USER_LEVEL). С учётом того, что существенной особенностью операций в среде выполнения программ СК является возможность изменения роли субъектов и объектов информационного взаимодействия, для контроля неизменности объектов предлагается использовать специальные механизмы идентификации контекста выполнения процессов.

На сетевом коммуникационном оборудовании стационарных суперкомпьютеров, рабочих станциях клиентов (операторов) и сервизных узлах суперкомпьютерного центра обработки данных устанавливаются средства криптографической защиты информации, средства антивирусной защиты, программно-аппаратные средства доверенной загрузки и средства защиты от несанкционированного доступа, межсетевые экраны и т.д. Для защиты передаваемых данных используются скремблеры и шифраторы. Бортовые супер-ЭВМ размешаются в специальных шкафах с замками. Несущие конструкции бокса в защищенном исполнении, используются кабели с экранированием. Поэтому на сервисных и клиентских хостах СК уровень защищенности максимально высокий. Единственными совсем незащищенными сегментами остаются вычислительные узлы (блоки) и инфраструктура взаимодействия вычислительных узлов с клиентскими и сервисными хостами, поскольку с учетом эксплуатационных и технических требований высокой производительности обработки, передачи данных по сети, асинхронности и параллельности выполняемых задач на них не устанавливают дополнительное ПО в виде средств защиты.

Процессорные устройства суперкомпьютеров могут функционировать в разных режимах: на уровне IPL в режиме хост-контроллер (одна управляющая ОС), «гнездовой» контроллер (nested virtualization host, несколько управляющих ОС на уровне IPL), виртуальный вычислительный узел многосокетной платы в реальном режиме (Direct IO computing node, один экземпляр гипервизора на уровне нулевого кольца защиты для группы виртуальных машин вычислительного кластера) или в режиме эмуляции с поддержкой запуска на одном сервере нескольких экземпляров задач (VT computing node, несколько гипервизоров на уровне 0 кольца защиты). Каждому режиму функционирования однозначно соответствует набор переменных Dom_id, s. С учетом значений системного бита s число уровней привилегий при обработке запросов в гипервизоре становится равным восьми.

Построена *логическая функция оценки безопасности Fi (R)*, где R = {x1 … x8} – входной вектор-параметр. При изменении контекста выполнения запроса происходит переключение между разными режимами, что отражается в наборе кортежа данных генеративных таблиц в виде восьми переменных x1, x2, x3, x4, x5, x6, x7, x8, которые задают функцию оценки безопасности состояния современной суперкомпьютерной системы как непротиворечащие требованиям политики безопасности.

В результате любой инициатор процесса доступа может использовать только разрешенные последовательности операций, признак которых задается в виде логической функции, которая определена на кортежах значений восьми переменных:

Fi = (Opcode, Dom_id, s, Ord, Context_type, Context_id, tcu, tr) (2),

где x1 = Opcode; x2 = Dom_id; x3 = s; x4 = Ord; x5 = Context_type; x6 = Context_id; x7 = tcu; x8 = tr; s – предикат, определяющий контекст выполнения процесса; Ord – предикат, задающий признак родительского или дочернего процесса; Context_type определяет изменения контекста выполнения процесса:

- Context_type = 1 (в двоичной кодировке 01) соответствует операциям чтения или записи в области памяти приложений;
- Context_type = 3 (в двоичной кодировке 11), осуществляются операции чтения или записи в привилегированную область памяти;
- Context_type = 2 (в двоичной кодировке 10), ошибка записи в буфер данных;
- Context_type = 0 (в двоичной кодировке 00) режим ожидания новых запросов, при этом не осуществляются операции записи данных.

tcu – переменные для контроля результатов выполнения запроса, параметр tr введен для контроля контекста выполняемых операций; Context_id – уникальный идентификатор запроса; Domain_id – идентификатор домена защиты; Opcode либо равен 0, если нет потока команд или пустая команда (NOP), либо 1, если содержит последовательность команд (!=NOP); M – базовое множество метаопераций, Opcode ∈ M.

Таким образом, существует упорядоченный набор кортежей переменных, который позволяет однозначно идентифицировать состояние как разрешенное или запрещенное для всех возможных изменений контекста операций в разных режимах функционирования процессоров (таблица 2). Предложенная модель операций позволяет оперативно построить отображение Ri → {1|0} как конъюнкцию простых предикатов, характеризующих состояния суперкомпьютерной системы при выполнении запросов.

На рисунке 1 приведена структура передаваемых пакетов в авторской модели безопасных операций при работе на недоверенной аппаратуре. Видно, что для корректной обработки запросов на уровне оборудования добавлены дополнительные поля:

Status – состояние процесса, B – признак блокировки, CF – контрольные биты для сверточных кодов.

| Opcode | Context_id | CF | Dom_id | S | Ord | Context_type | Status | B | Tr |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |

**Рисунок 1 – Вид тегированной структуры пакета запросов**

*Критерии идентификации угроз* на наборах кортежей логических переменных x1, x2, x3, x4, x5, x6, x7, x8 приведены в таблице 3.

Сравнение моделей безопасных операций с точки зрения реализаций функций управления и разграничения доступа приведено в таблице 4.

Во всех существующих традиционных моделях безопасных операций не разработаны и не формализованы функции контроля полномочий субъектов и доступа к объектам на всех уровнях иерархии СК, а также функции контроля контекста и тайминга выполнения операций.

Проблема «больших данных» приводит к тому, что нельзя пренебрегать малыми разрядами кодируемых данных, поскольку изменения в небольшом сегменте могут привести к переносу разрядов и появлению значащих битов в последовательности запросов, обрабатываемых процессорным устройством.

Для контроля границ адресации и смещения в конвейере обрабатываемых директив и блокирования выполнения «ложных запросов» генерируемые таблицы формируются на этапе подготовки задачи и хранятся в специальном регистре t_reg. Сначала передается стандартная процедурная составляющая – опкод инструкций (набор кода данных и кода команд, модификаторов и флагов условных переходов). Затем в структуру кадра (фрейма) каждого запроса пользователя вводятся восемь дополнительных регистровых полей (префикс).

Предложено процессы обработки запросов декомпозировать на 8-уровневую иерархическую структуру, представляющую собой конвейер, который имеет восемь интерфейсных уровней. На основе предложенной декомпозиции модель безопасных операций можно конструктивно представить с помощью мультиграфа запросов, который описывает разрешенные механизмы инициализации процессов доступа к прикладным и системным информационным ресурсам.

**Таблица 2 – Соответствие набора переменных Dom_id, s уровню привилегий и режиму функционирования процессора**

| Dom_id | s | Режим функционирования процессора | Соответствие уровню иерархии обработки в гипервизоре | Уровни привилегий |
|---|---|---|---|---|
| 00 | 0 | хост-контроллер оборудования (SMM-режим Bare Metal гипервизора – самый привилегированный) | Уровень S8 | IPL (контроллер материнской платы, уровень инструкций процессора) |
| 00 | 1 | «гнездовой» контроллер оборудования (аппаратный гипервизор – монитор виртуальных машин) | Уровень S7 | |
| 01 | 0 | Direct IO computing node (управляющая ОС на физическом сервере в реальном режиме) | Уровень S6 | Kernel_level (нулевое кольцо защиты, ядро управляющей ОС) |
| 01 | 1 | VT computing node (управляющая ОС на физическом сервере в режиме эмуляции) | Уровень S5 | |
| 10 | 0 | Менеджер ресурсов в режиме прямого доступа к оборудованию | Уровень S4 | Supervisor_level (первое кольцо защиты, взаимодействие ядра ОС с физическим оборудованием) |
| 10 | 1 | Менеджер ресурсов среды виртуализации (пара виртуализация) | Уровень S3 | |
| 11 | 0 | Управляющая ОС кластера виртуальных машин | Уровень S2 | Application_level (третье кольцо защиты, уровень приложений) |
| 11 | 1 | Гостевые «гнездовые» ОС виртуальных машин | Уровень S1 | |

**Таблица 3 – Критерии идентификация угроз на наборах кортежей логических переменных x1, x2, x3, x4, x5, x6, x7, x8**

| x1 | x2 | x3 | x4 | x5 | x6 | x7 x8 | Пояснение |
|---|---|---|---|---|---|---|---|
| !=NOP | 0X | X | X | 1 | != 0 | XX1X X1 | Осуществляется попытка злоумышленника изменить конфигурацию хостовой ОС физического сервера |
| !=NOP | 0X | X | X | -1 | ! = 0 | XX1X X1 | Осуществляется попытка злоумышленника перехвата обращений хостовой ОС к драйверам физических устройств |
| !=NOP | 1X | X | X | X | != 0 | 0101 01 | Ресурс занят приложением, штатный режим запуска задачи пользователем или администратором, асинхронный режим доступа к ресурсам |
| !=NOP | 01 | X | X | X | != 0 | 0101 01 | Ресурс занят приложением, штатный режим запуска задачи хостовой ОС, асинхронный режим доступа к ресурсам |
| !=NOP | 01 | X | X | X | != 0 | 0100 10 | Ресурс занят приложением, штатный режим запуска задачи хостовой ОС, синхронный режим доступа к ресурсам |
| !=NOP | XX | X | X | X | 0 | XXXX XX | Попытка скрыть процесс-поток в дескрипторных таблицах хостовой ОС, присвоив статус «System Idle Process» |
| !=NOP | 00 | X | X | X | != 0 | XX1X X1 | Попытка запуска недоверенного модуля на уровне IPL |

**Таблица 4 – Сравнение моделей безопасных операций с точки зрения реализаций функций управления и разграничения доступа**

| **Название модели** | **Изоляция процессов, защита на уровне доменов** | **Контроль доступа к объектам на всех уровнях иерархии** | **Контроль полномочий на всех уровнях иерархии** | **Контроль контекста выполнения операций на уровне процессора и контроллера памяти** | **Контроль тайминга операций** |
|---|---|---|---|---|---|
| Авторская модель безопасных операций | 8 доменов защиты и механизмы верификации на каждом уровне доменной защиты | Число уровней иерархии субъектов однозначно соответствует числу уровней иерархии объектов защиты | Учтены все режима работы системы. 8-уровневая «песочница» | Введены новые параметры:<br>Delta<br>Diff<br>Context_id<br>Context_type<br>Ord<br>Dom_id | Введены новые параметры:<br>TR<br>TCU<br>Opcode |
| Модель Грэхама-Деннинга | Нет | Нет | Нет | Нет | Нет |
| Модель Кларка-Вильсона | Нет | Нет | Нет | Нет | Нет |
| Субъектно-ориентированная модель | Нет механизмов верификации на каждом уровне доменной защиты | Контроль только на основе меток | Контроль на основе мандата | Нет | Нет |
| Модель Take-Grant | Нет механизмов верификации. на каждом уровне доменной защиты | Нет | Нет | Нет | Нет |

**Продолжение таблицы 4**

| | | | | | |
|---|---|---|---|---|---|
| ЭМЗАС-модель Воронежский институт МВД, ФСТЭК России | Не предложены критерии обнаружения угроз | Контроль только на основе меток | Контроль на основе мандата и элементы ролевой ПБ | Нет | Нет |
| Модель Росатома | Не предложены критерии обнаружения угроз | Контроль только на основе меток | Контроль на основе мандата и элементы ролевой ПБ | Нет | Нет |

В результате предложенной формализации описание скрытых угроз сводится к введению контекстно-зависимых переходов в мультиграфе запросов G = G(к) (рисунок 2).

Характеризуем его математической моделью дискретной динамической системы:
x(t +1) = F(x(t); p) = F(x(t); k(t), v) с начальным условием x(0) = x0, q – число уровней квантования аргументов функции

F: x(t) = (x1(t), x2(t),..., xn(t)) (3),

где к = (к1, к2,..., кn) – «управляющий» параметр формализован в виде набора кортежей;
v = {M} – набор метаопераций, т.е. поток входных данных в виде опкода;
t0 – время начала выполнения (точка отсчёта);
(t0 + k * Δ) – длительность выполнения k инструкций в процессорных тактах;
Ui – i-ая инструкция штатного ПО на Si уровне;
Vj – j-ая инструкция стороннего агента;
nm – число инструкций в обработчике Si на разных интерфейсных уровнях после сборки команд непосредственного сценария выполнения исходящих директив;
p – вероятность того, что при выполнении инструкции трассы произойдет переключение из одного режима функционирования процессорного устройства в другое (проход по нижней дуге); p = pi + δp, где pi – вероятность переключения в i-ый режим работы, а δp – корректирующий параметр, учитывающий вероятность задержки в распространении сигналов при изменении режима работа аппаратуры (тактовой частоты процессора, скорости кэширования, тактовой частоты работы памяти и т.д.);
q – вероятность выполнения инструкции трассы без изменения контекста выполняемых операций (проход по верхней дуге).

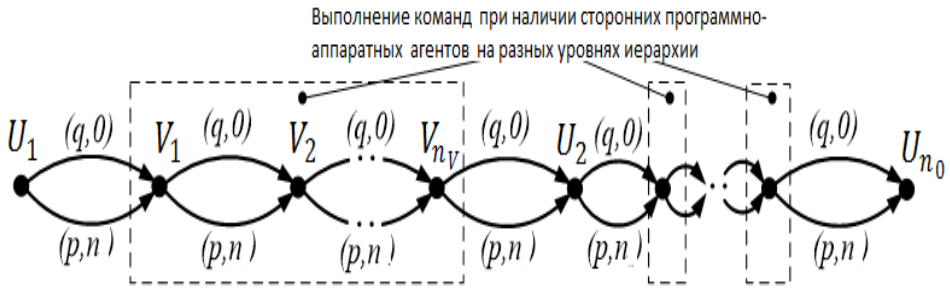


**Рисунок 2 – Мультиграф запросов G(k)**

Неоднозначность обусловлена тем, что выполнение программ на уровне объектов гостевых и управляющих ОС в недоверенной среде не эквивалентно изменению состояний компонентов гипервизора, обрабатывающих запросы пользователей на выделение вычислительных ресурсов СК при взаимодействии с физическим оборудованием.

В системе наблюдаются переходные процессы. Внутренний цикл работы процессора на аппаратном уровне определяется временными интервалами (t – периоды синхронизации). Введённый автором дополнительный уровень доменной защиты S8 – это уровень, на котором осуществляется верификация и контроль сборки команд непосредственного сценария выполнения исходящих директив.

Значения функций фильтрации Bf = {1/8, 1/4, 3/8, 1/2, 5/8, 3/4, 7/8}. Это набор всех интервальных значений, кратных 1/8. Интервально-временные ограничения обусловлены особенностью аппаратной реализации управления режимами функционирования процессорных устройств, о чем уже упоминалось ранее. Алгоритм вычисления дескриптора оценки безопасности состояний адаптирован к типу конфигурации СК и потоку обрабатываемых данных.

Суть новой модели безопасных операций состоит в следующем. Выдаваемые запросы изначально связываются с некоторой информационной структурой, называемой тегом.

Происходит планирование действий для каждого запроса на всех интерфейсных уровнях, а также фиксация информации о контексте его выполнения. По мере продвижения запроса через уровни в теге накапливается информация в виде межуровневой трассы.

Работа с тегами запросов на уровнях защиты производится агентами гипервизора.

Повышение уровня привилегий с одного уровня на другой в одном режиме функционирования процессора осуществляется за счет изменения бита системности s. При передаче управления после системного вызова уровень привилегий понижается до уровня привилегий того уровня, на котором был сформирован запрос в виде исходящих директив.

Не допускается «перескакивать» через уровни. При попытке получить доступ из непривилегированного уровня в одном режиме работы процессора к привилегированному уровню в другом режиме работы процессора происходит изменение двух значащих разрядов в поле tr на 11. Отслеживается также попытка обращения приложений к данным из одного режима работы к данным в другом режиме работы процессора. При этом происходит изменение двух значащих разрядов в поле tr на 00.

Осуществляются мониторинг и контроль выполнения переключений и передачи управления между директивами при выполнения операций: значащие четыре разряда поля tcu – это статус выполнения процесса, в поле tr значение 01 сигнализирует о том, что идет переходный процесс (дуги между узлами), 10 – переходного процесса нет.

При изменении хеш-значения в указанной логической иерархической структуре меняются идентификация вершин трассы и нумерация маршрута прохождения, что свидетельствует о подозрительной активности в системе. С учетом квазидетерминированности системы возможно снижение размерности решаемых задач исследования в виде перехода от сложных скрытых марковских моделей к упрощенной модели (марковского процесса с дискретными состояниями и непрерывным временем на примере мультиграфа состояний с учетом вероятных угроз атаки).

*Критерии верификации* небезопасных операций, реализованные в методе реактивной защиты, показаны в таблице 5.

**Таблица 5 – Критерии верификации небезопасных операций на структурах Крипке с использованием модальных выражений темпоральной логики CTL**

| Тип угроз | Критерии верификации небезопасных операций (примеры структур Крипке) | Комментарии |
|---|---|---|
| Угрозы НСД до загрузки ОС и во время загрузки ОС | AG [S7 $\Rightarrow$ AX[A(Ord = False U S8) $\vee$ AG $\neg$L8] &&<br>FG (Start_mon & Ord =False) | Между уровня иерархии обработки запросов (команд) S7 и S8 всегда выполняется свойство Ord = 0, поскольку на данном уровне иерархии функционирования системы здесь не запускаются любые порожденные процессы, а только инициализирован и работает один базовый процесс – верификатор команд.<br>При включении ЭВМ первым инициализируется и запускается доверенный модуль верификатора команд.<br>С момента запуска (событие Start_mon), всегда выполняется условие Ord=0.<br>Если не выполняется хотя бы одно из условий, операция блокируется. Администратору отправляется оповещение. |
| Угрозы НСД после загрузки ОС | If $\neg$EF (delta > 1) &&<br>Diff{Priv(si), Priv(si+1)} >0,<br>delta = max{Priv(si), Priv(si+1)} – Priv(si) = 1; else Diff{Priv(si), Priv(si+1)} < 0, то delta = Priv(si+1) – min{Priv(si) = 1,<br>else delta = 0. | Не существует такого режима работы для квантора пути w, при котором изменение delta-параметра превысит значение 1 при переходе из si в si+1.<br>Верификатор команд реализует функции защиты при обработке запросов контроллером аппаратной транзакционной памяти и при выполнении последовательности команд в исполнительном регионе процессора. |

**Продолжение таблицы 5**

| | | |
|---|---|---|
| Угрозы отказа в обслуживании с использованием средств срытого информационного воздействия, в результате внешних дестабилизирующих их воздействий по каналам коммуникации, некорректного выполнения операций, неправильных действий оператора или администратора | AG (process_is_on ⇒ P Hyper_Permission, delta) && AG (req ⇒ (start U ack)) && ¬F terminate (AG si & Context_type = 2 & tr = 0 OR tr = 3 ‖ B = 1) | В любом режиме, прежде чем запустится новый процесс, обязательно предварительно должна быть получена санкция со стороны гипервизора.<br>Во всех режимах, требующих изменения привилегий для запуска процесса, после того, как запрос req установится, он никогда не будет обработан, пока на него не придет подтверждение.<br>Условие подтверждения delta = 1.<br>Для всех состояний si на всех траекториях с ошибками или при условии блокировки ресурса запрос принудительно завершается. |
| Угрозы внедрения вредоносных программ в гостевых и хостовых ОС | G delta (tr & ¬tr) – && ¬F descrypt (hcode_TCU=False) – && ¬F terminate (AG si & Context_type = 2 & tr = 0 OR tr = 3 ‖ B = 1) | Всегда будет вычисляться функция delta для тех случаев, когда в системе не возникают ошибки. Если значения tr = {00, 11}, то вычисление не проводится, запрос вообще не обрабатывается и удаляется. В остальных случаях, когда событие 10 – начинается переходный процесс, событие 01 – завершается переходный процесс завершился, проводится контроль на соответствие уровня доступа к запрашиваемым данным с уровнем привилегий инициатора доступа.<br>Никогда не проводится вычисление дескриптора оценки безопасности для тех состояний, когда нет активных задач, то есть два старших бита поля TCU (спецификатор hcode_TCU) обнулены. Два младших бита TCU (спецификатор lcode_TCU) кодируют состояние выполнения.<br>Бит B – состояние блокировки (если бит равен 1, то ресурс занят).<br>Для всех состояний si на всех траекториях с ошибками запрос принудительно завершается. |
| Угрозы внедрения по сети вредоносных программ гостевых и хостовых ОС | G delta (tr & ¬tr) – && ¬F descrypt (hcode_TCU=False) – && ¬F terminate (AG si & Context_type = 2 & tr = 0 OR tr = 3 ‖ B = 1) | |

Если сравнивать с существующими на сегодня классическими методами реактивной защиты на основе сигнатурного анализа, методами реактивной защиты на основе поведенческого анализа и эвристическими методами реактивной защиты, то в них *не реализованы функции защиты и верификации при обработке запросов контроллером аппаратной транзакционной памяти и при выполнении последовательности команд в исполнительном регионе процессора*, поэтому они не способны выявлять и блокировать угрозы ИБ на всех уровнях иерархии субъектов и объектов СК.

**В четвертой главе** разработаны метод реактивной защиты и метод реконфигурации среды выполнения программ проактивной защиты на основе применения маркеров и интервально-временных ограничений в соответствие с оценкой безопасности в виде модальных правил темпоральной логики CTL и реализован набор файлов конфигураций системного ПО. *Метод реактивной защиты,* основанный на виртуализации процессов, если вычисленный дескриптор состояния попадает в зону «риска», включает в себя алгоритмы вычисления дескрипторов оценки безопасности состояний и идентификации угроз на основе маркировки состояний выполнения запросов СК. Вычисление результирующей свертки осуществляется на основе атрибутов протекающих процессов с заданной глубиной (масштабируемостью). Весовой коэффициент защиты определяется как разность между исходным (эталонным) значением хеша и полученным после прохождения пакета запросов и вычисления свертки. Для количественной оценки величины возмущений используется относительный показатель e = $(C_u - C_a)/ C_a$ , где $C_u$ – состояние до атаки, $C_a$ – состояние после атаки. Этот параметр используется в методе в качестве корректирующего параметра для обучения на каждом уровне (слое) иерархии обработки запросов.

Пронумерованы все узлы мультиграфа. Для каждого процесса и подпроцесса обработки запроса уникальный хеш вычисляется на этапе инициализации и записывается в генерируемую (генеративную) таблицу гипервизора. Каждый процесс пронумерован: если нет дочерних процессов, то бит Ord = 0. Нумеруются все вершины подграфа родительского процесса с присвоением новому узлу уникального идентификатора в виде хеша.

Вместо классического подхода в виде скрытых марковских процессов с использованием алгоритма Баумана-Уэлча предложено использовать вычисления траекторий на основе темпоральной логики CTL, заданных на структурах Крипке с набором вероятностных значений оценки защищенности. Вычисление доверительной вероятности производится по формуле Корнфельда (4), представляющей собой убывающую геометрическую прогрессию при значениях n от 0 до + ∞, и заключается в выборе доверительного интервала в пределах от минимального до максимального результата измерений. Пусть $x_1, x_2, .., x_n$ – результаты измерений. Интервал от $\tilde{x} - \Delta x$ до $\tilde{x} + \Delta x$ – доверительный интервал, где $\tilde{x}$ – средняя арифметическая взвешенная,

$\Delta x = \frac{1}{2} * (x_{MAX} - x_{MIN})$.

Доверительная вероятность p = $1 - \Sigma \left(\frac{1}{N}\right)^{n-1}$ , 1 …n (4),

где N – число режимов работы процессора.

Если в системе два режима функционирования: R-режим и S-режим, то доверительная вероятость p = 0,66666666, q = (1 – p) = 0,33333333. Контекст изменения операций – это изменения значений значащих разрядов в кортежах логических переменных при проходе запроса с первого по восьмой уровень иерархии.

В работе в виде модели выполнения операций СК применён формализм мультиграфа, представляющего собой дерево. Стартовая точка – это вершина древовидной структуры, описывает контроллер транзакционный памяти, который напрямую взаимодействует с верификатором команд. В случае суперкомпьютерных систем нельзя пренебрегать разрядами с точностью до восьмого знака. Для *стационарных суперкомпьютеров* с учетом восьми уровней защиты (N = 8) p = 0,88888889, q = (1 – p) = 0,11111111.

Следовательно, при такой конфигурации стохастический процесс перехода из одного режима функционирования в другой под внешним специальным воздействием или в результате проведения атак становится квазидетерминированным. Доверительная вероятность равна почти 0,9. Показатель защищенности компонентов среды выполнения программ достигает максимума, когда система перестает быть уязвимой к любым видам воздействий и типам атак. Профиль защиты и полные расчетные данные для всего набора конфигураций в зависимости от типа СК приведены в таблице 6. Вычисления с точностью до 8-го знака выполняются в том случае, если используем стационарные СК.

В случае применения *бортовых супер-ЭВМ* для ускорения работы и оптимизации вычислений целесообразно пренебречь погрешностью при выполнении операций над данными в пользу высокой производительности в режиме реального времени и базового (минимального) уровня защиты. Например, число 0,88888889 представляет собой приближенно периодическую дробь 0,(8)n. Тогда мы можем проводить вычисления для мобильных систем с точностью до первого разряда после запятой, в зависимости от типа архитектуры процессора варьируется и число используемых интерфейсов N, влияющих на мощность пространства вычислений.

**Таблица 6 – Профиль защиты и набор конфигураций для разного класса СК**

| **Класс Суперкомпьютеров / Максимальное количество уровней иерархии обработки запросов (маркеры привилегий)** | **Доверительная вероятность уровня защищенности по формуле Корнфельда p** | **Вероятность проведения успешной атаки q = (1 – p)** | **Максимальное количество доменов защиты N (создание изолированной программной среды)** |
|---|---|---|---|
| Стационарные суперкомпьютеры: 1 тип – малый кластер<br>6 | 0,8-0,83 | 0,2-0,17 | 4 или 5<br>(средний уровень защиты) |
| Стационарные суперкомпьютеры: 2 тип – средний кластер<br>7 | 0,857-0,875 | 0,143-0,12 | 6 или 7<br>(высокий уровень защиты) |
| Стационарные суперкомпьютеры: 3 тип – стратегический класс<br>8 | 0,9 | 0,1 | 8<br>(максимальный уровень защиты) |
| Бортовые супер-ЭВМ<br>От 3 до 5 | 0,75-0,8 | 0,25-0,2 | От 2 (минимальный уровень защиты)<br>до 3-4 (базовый уровень защиты) |

Контроллер транзакционной памяти в связке с верификатором команд реализует изолированное мультидоменное адресное пространство, которое представляется в виде неперекрывающихся областей памяти. Поскольку у нас 8 уровней иерархии обработки запросов, то блок разбит на восемь подмножеств детализации уровней возможных состояний, обозначенных S8, …, S1. Последний уровень корневой структуры мультиграфа представлен агентами гипервизора (листья графа), через которые происходит связь с внешней средой. Продвижения на каждый следующий уровень – это более высокий уровень абстракции описания обработки запросов, переход от нижнего уровня спецификации к верхнему. Каждое состояние может иметь не одну, а множество цепочек – продолжений, и является корнем своего дерева историй (вычислений).

*Метод реконфигурации среды выполнения программ проактивной защиты* основан на методах темпоральной логике для проверки истинности принимаемых решений на каждой возможной интерпретации (структуре Крипке) с учетом специфики СК в виде временной сложности, связанной с параллельностью вычислений, и пространственной сложности, обусловленной большим количеством ядер процессоров и структурных связей между ними. Базовый процесс инициализуется значением context_id (исходная вершина графа для старта вычислений). Каждый процесс нумеруется уникальным хеш-значением.

Изменение в поле Ord для каждого процесса сигнализирует о появлении уже дочерних подпроцессов в рамках базового процесса. Хеш вычисляется рекурсивно для всех процессов (подпроцессов). В итоге получается результативное значение для штатного измерения трассы прохождения запроса (на основе прошлого опыта). В процессе работы идет обучение системы. Каждая новая конфигурация классифицируется и в будущем распознается с учетом характерного набора маркеров.

Темпоральная логика учитывает мультиветвления по времени и историю порождения разных конфигураций. У разных конфигураций – разные уровни привилегий базового и наследованных от него дочерних процессов. В классических средствах защиты ОС задается только *ссылка на объект*. Автором предложено вычислять хеш для каждого процесса обработки.

В таблице 7 приведено сравнение методов проактивной защиты. Ни один из существующих методов проактивной защиты не адаптирован для решения задач идентификации и блокирования угроз ИБ с учетом специфики суперкомпьютеров.

Наилучшие показатели защищенности, количество реализованных функций безопасности демонстрирует авторский метод.

**В пятой главе** предложена и разработана методика тестирования уровня защищенности и реализован алгоритм идентификации угроз ИБ на основе таблиц правил ПБ и набора маркеров.

Разработаны два варианта исполнения: программный и программно-аппаратный. Программная реализация «Альфа-монитор» состоит из проксирующих модулей и модуля верификации команд гипервизора, программных агентов сбора метрики приложений и мониторинга событий безопасности. Аппаратная составляющая программно-технических решений представляет собой устройство в защищенном исполнении.

Загрузка/выгрузка контрольных образцов вредоносного ПО производится в режиме эмуляции. Длина каждого цикла измерения равна восьми этапам обработки. Параметры выполнения трасс на основе счетчика команд вносятся в базу данных для дальнейшего обучения. Циклический счетчик фреймов реализован в аппаратуре контроллера материнской платы в режиме реального времени, чтобы минимизировать побочные и неконтролируемые прерывания, которые маскировали истинное время выполнения системных команд.

**Таблица 7 – Сравнение методов проактивной защиты**

| **Название метода** | **Параметр учета переходов процессов** | **Признак системности** | **Признак блокировки операций** | **Контроль контекста и тайминга выполнения операций** |
|---|---|---|---|---|
| Авторский метод проактивной защиты<br>*Показатель гарантированной защищенности*<br>*P = 0,9* | Да | Контроль со стороны верификатора команд выполнения операций процессором и контролером транзакционной памяти | Да | Реализованы расширенные функции идентификации и верификации |
| Эволюционный метод проактивной защиты на основе генетических алгоритмов<br>*Показатель гарантированной защищенности*<br>*P = 0,5* | Нет | Нет | Нет | Нет |
| Метод проактивной защиты на основе прогнозирования в виде экстраполяции данных<br>*Показатель гарантированной защищенности*<br>*P = 0,5* | Нет | Нет | Нет | Нет |
| Метод проактивной защиты на основе скрытых марковских цепей<br>*Показатель гарантированной защищенности*<br>*P = 0,6* | Нет | Только регистрация изменения системного бита | Нет | Нет |

Методика тестирования уровня защищенности в виде проведения формирования набора угроз включала в себя набор из 3000 тестовых воздействий, реализуемых на разных уровнях иерархии обработки запросов в многоядерных процессорных системах. В ходе генерации внешних дестабилизирующих воздействий, регистрировались значения нужных переменных в буфере запросов. Выбирались взвешенные значения полученных данных в каждом раунде. Полученные результаты подвергались регрессионному анализу.

Методика тестирования уровня защищенности основана на следующих принципах и подходах:

1. На основе значений функции оценки безопасности состояний Fi, аргументы которой заданы в виде конъюнкции предикатов из восьми логических переменных x1, x2, x3, x4, x5, x6, x7, x8.
2. На основе выборочных центральных моментов ожидания u 8-го порядка: $Z = \{\vec{x}_n : u(\vec{x}_n) \geq \mu\}$.
3. На основе выборочной дисперсии $\hat{\sigma}^2$: $Z = \{\vec{x}_n : \hat{\sigma}^2(\vec{x}_n) \geq d\}$.
4. На основе длины вариационного ряда $\hat{l} : Z = \{\vec{x}_n : \hat{l}(\vec{x}_n) \geq w\}$.

Обнаружение осуществляется на основе списка демаскирующих событий по значениям траекторий вычислений темпоральной логики CPL на структурах Крипке, по временным параметрам (изменение длины трассы выполнения инструкции) и величины энергозартат на выполнение инструкций в пДж. На одну операцию в процессоре тратится порядка 29-45 пДж (технология сборки 40-22 нм). Частое переключение между режимами функционирования и перезапуск задач на всем линейном функциональном устройстве требует энергозатрат порядка 1,1-19 мкДж, что позволяет обнаружить нелегитимное ПО или работающее закладочное устройство. В момент его работы наблюдается «резкий» всплеск энергетической активности по усредненным показателям за длительный интервал наблюдений. Из выбираемых характеристик большого числа тестовых измерений в качестве пороговых значений $\mu, d, w$ выбираются те, сумма вероятностей ошибок 1-го и 2-го рода которых минимальна. В качестве порогового значения по энергоэффективности выбран параметр среднего значения e > 1100 пДж.

Процедура поиска разных классов вредоносного ПО представляет собой цикл, в котором анализируются списки запросов, на основе значения функции оценки состояния Fi: если Fi = Да, процесс добавляется в список разрешенных, если Fi = Нет, формируется список запрещенных процессов. В результате работы алгоритма создается база данных вредоносного программного обеспечения, которая периодически обновляется.

На рисунке 3 показано, что при количестве n >= 86 из 100 обучающих выборок обеспечивается стабильное обнаружение с критически минимальными ошибками 1-го и 2-го рода. При увеличении выборок и интервала наблюдения по времени наблюдается устойчивое снижение: значение ложных срабатываний стремится к нулю. При такой конфигурации, когда число уровней иерархии N = 8, выполнение контекстно-зависимых операций становится квазидетерминированным с доверительной вероятностью приблизительно 0,9, а изменения в работе компонентов СК, вызываемые дестабилизирующим воздействием со стороны вредоносного ПО, меньше 0,1.

Таким образом, найден инвариант, когда система перестает быть уязвимой к компьютерным атакам. В таблице 8 и таблице 9 приведены результаты стендовых испытаний и сравнения функциональных возможностей четырех СЗИ: Group-IB Polygon, Kaspersky KATA, PT Security Sandbox (на основе марковских процессов с использованием алгоритма Баумана-Уэлча), авторский продукт «Альфа-монитор» (с использованием алгоритма “маркерного” сканирования).

Обобщая все сказанное выше, можно сделать вывод о том, что показатели защищенности суперкомпьютеров, на которых установлен защищенный мультидоменный гипервизор, наилучшие, а требования к вычислительным ресурсам в 5-6 раз меньше, чем у существующих технологических решений на рынке СЗИ.

Использование восьми кластеров для эффективного обнаружения вредоносного кода значительно сокращает расходы на реализации программно-технического решения.

Испытания на экспериментальном стенде показали минимальные потери производительности – менее 6-7 процентов.

**Таблица 8 – Результаты измерений**

| **Класс СК** | **Количество интервальных ограничений фильтрации** | **Количество уровней иерархии операций** | **Вероятность ошибки идентификации угроз (взвешенные усредненные значения)** | |
|---|---|---|---|---|
| | | | **I рода** | **II рода** |
| 1. Ботовые супер-ЭВМ (сверхлегкие ядра) | 3 | 4 | 0.01 | 0,012 |
| 2. Малый промышленный кластер (легкие ядра) | 4 | 5 | 0.001 | 0, 003 |
| 3. Средний суперкластер (средние ядра) | 6 | 7 | 0,0008 | 0,0007 |
| 4. Суперкластер стратегического класса (тяжелые ядра) | 7 | 8 | 0,000035 | 0,000045 |

**Таблица 9 – Результаты тестирования СЗИ**

| **Название СЗИ** | **Число кластерн. зон для обучения** | **Макс. число доменов защиты** | **Число успешных распознаваний** | **Погрешность** | **Эффективность** | **Потери производ.** |
|---|---|---|---|---|---|---|
| Group – IB Polygon | 50 | 2 | 5 из 100 | 0,55 | 0,05 | 35-40 % |
| Kaspersky KATA | 60 | 3 | 4 из 100 | 0,6 | 0,04 | 40-46 % |
| PT Security Sandbox | 56 | 3 | 6 из 100 | 0,53 | 0,06 | 25-30 % |
| Альфа-монитор | 8 | 8 | 86 из 100 | 0,0139 | 0,86 | 6-7 % |

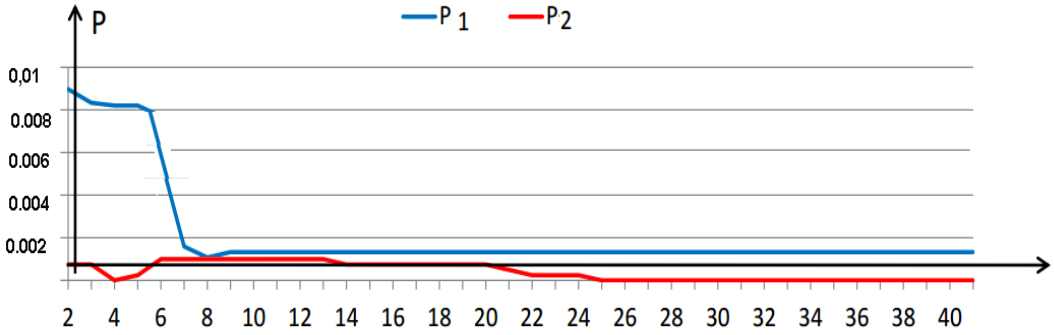


**Рисунок 3 – Зависимость вероятности ошибок 1-го и 2-го рода от количества обучающих кластеров**

**В заключении** сформулированы основные выводы, перечислены полученные в работе результаты.

**В приложениях** указаны Патенты на изобретения, свидетельство о регистрации программы ЭВМ, приведено описание схемы и набора программно-инструментальных средств экспериментального стенда, Акты внедрения (реализации) и чертежи.

**Рекомендации по применению** включают в себя указания по использованию применению методов и методики тестирования уровня защищенности СК. Научные и практические результаты могут быть использованы для широкого класса систем с гибкой конфигурацией окружения и контекстом вызовов сервисов, сбором метрики приложений на основе мультитредовой архитектуры с управлением потока данных.

**В качестве перспектив дальнейшей разработки** тематики следует указать исследования, связанные с развитием моделей описания информационных процессов и улучшения показателей идентификации вредоносного ПО. Также возможно использование описанных в работе моделей и методов в целевых программах и опытно-конструкторских работах силовых ведомств при разработке перспективных информационных систем, ввод в промышленную эксплуатацию суперкомпьютера «Ангара» на базе отечественного процессора J7 в рамках национального проекта по импортозамещению.

## ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ И ВЫВОДЫ

1. Разработаны теоретические и научно-методические принципы защиты стационарных и бортовых суперкомпьютеров с использованием средств виртуализации, основанные на построении и формализации универсальных и равномерных функций оценки безопасных состояний СК для заданных классов операций, что, в отличие существующих аксиоматик в классической теории информационной безопасности, позволяющие решить научную проблему супервентности. При этом получены важные теоретические выкладки. Доказана теорема о равномерной перечислимости функций СК.
2. Разработана модель угроз целостности среды выполнения процессов, основанная на новой парадигме написания правил политики безопасности, что, в отличие от существующих методик ФСТЭК России и Росатома, позволяет учесть специфику работы стационарных и бортовых суперкомпьютеров. Вместо классической связки «субъект, объект, предикат» реализована новая парадигма написания правил политики безопасности и заданы новые сущности – «субъект», «объект» и «дескриптор оценки безопасности состояний»: для каждой i-ой угрозы вычисляется значение функции оценки безопасности состояний, аргументы которой заданы в виде конъюнкции предикатов из восьми логических переменных, субъектами являются гостевые и управляющие ОС, а объектами – компоненты гипервизора и контроллера транзакционной памяти.

3. Разработана модель безопасных операций, основанная на декомпозиции информационных процессов в виде 8-уровневой иерархической структуры, что, в отличие от классических моделей безопасности дискреционного, мандатного, ролевого управления доступом, логического управления доступом и информационными потоками (ДП-моделей), в том числе иерархическим представлением мандатной сущностно-ролевой ДП-модели, позволяет идентифицировать и блокировать новый класс угроз, связанных с неоднозначностью состояний выполнения прикладных и системных программ на стационарных и бортовых суперкомпьютерах. Сформулировано условие разрешимости проблемы установки логического соответствия (супервентности) между изменениями программ среды исполнения СК и изменениями компонентов аппаратуры: если число уровней иерархии равно восьми, то процессы наблюдаемы на всех интерфейсных уровнях, любые трансляции операций гипервизором становятся безопасными.

4. Разработан и исследован метод реактивной защиты стационарных и бортовых суперкомпьютеров, основанный на виртуализации среды выполнения процессов, что, в отличие существующих классических методов управления доступом в изолированной программной среде, позволяет вычислять значения дескрипторов и задавать методы их обработки – get, set, delete и т.п.: вид характеристических функций при анализе траектории вычислений на структурах Крипке зависит от контекста входных данных и типа конфигурации СК. Ошибки 1-го и 2-го рода могут возникать на локальном i-ом уровне, но они детектируются и исправляются на уровне системной задачи анализа контроля целостности поступающей информации с датчиков со всех уровней иерархии обработки запросов**.**

5. Разработан и исследован метод реконфигурации среды выполнения программ проактивной защиты стационарных и бортовых суперкомпьютеров, основанный на парадигме темпоральной логики для проверки истинности принимаемых решений на структурах Крипке, что, в отличие от существующих классических методов мониторинга событий безопасности с использованием булевой логики, позволяет адаптировать число интерфейсных уровней к типу конфигурации СК и потоку обрабатываемых данных в режиме реального времени. Определены два направления реализации метода:

- для стационарных суперкомпьютеров заданы три конфигурации: число уровней защиты N от пяти до восьми. Предельное значение доверительной вероятности (при N = 8) приближается к 0,9. Показатель защищенности компонентов среды выполнения программ достигает максимума, когда система перестает быть уязвимой к любым видам воздействий и типам атак;
- для бортовых супер-ЭВМ задана конфигурация минимальной защиты, в которой число уровней N равно четырем. Доверительная вероятность равна 0,8. Таким образом, при уменьшении числа доменов защиты показатель защищенности компонентов среды выполнения программ по-прежнему остается высоким;
- показатель защищенности для традиционных СЗИ равен 0,5-0,6.

6. Разработана методика тестирования уровня защищенности стационарных и бортовых суперкомпьютеров, основанная на алгоритме “маркерного” сканирования, что, в отличие от современных методик, позволяет снизить затраты на использование вычислительных ресурсов для обучения и корректного распознавания при использовании требуется восемь обучающих доменов, поддерживаются любые форматы исполняемых файлов), снизить количество ошибок и повысить эффективность идентификации атак и угроз. Традиционные методики и алгоритмы требуют не менее пятидесяти обучающих доменов, при этом поддерживается только один PE-формат исполняемых файлов. Следовательно, по сравнению с внедренными промышленными решениями требования к вычислительным ресурсам при реализации алгоритма “маркерного” сканирования в 5 – 6 раз меньше. Экспериментальные исследования показали, что не менее чем в 86 из 100 обучающих выборок при использовании алгоритма “маркерного” сканирования ошибки 1-го и 2-го рода

не превышают 0,014. При увеличении выборок и интервала наблюдения по времени наблюдается устойчивое снижение: значение ложных срабатываний стремится к нулю. Для традиционных СЗИ во всех обучающих выборках (100 из 100) присутствуют ошибки 1-го и 2-го рода, которые превышают пороговое значение 0,5. Эффективность обнаружения авторской методики на 86 процентов выше по сравнению с классическими подходами.

7. Разработаны и запатентованы программно-технические решения в виде многомодульного защищенного мультидоменного гипервизора, основанные на разработанных моделях и методах, что, в отличие существующих сертифицированных гипервизорных решений, позволяют получить наилучшие показатели производительности, показатели защищенности и не допускают аварийных завершений критических процессов из-за компьютерных атак. Порог потери производительности при использовании комплекса верификации менее 6-7 процентов. Если количество измерений, получаемых с датчиков измерений на каждом уровне «песочницы», равно восьми, то показатель погрешности вычислений e = 0,0139. Подсистема обеспечения информационной безопасности реализована для российских суперкомпьютерных платформ семейства «Ангара» ЕС1740, китайских суперкомпьютеров серии Tian-he/CT-2, японских суперкомпьютеров серии Tsubame 3.0.

## СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

### В рецензируемых журналах из перечня ВАК


1. Моляков, А. С. Исследование скрытых механизмов управления задачами ядра Windows NT 5.1 / А. С. Моляков // Известия ЮФУ. Технические науки. – 2007. – № 4(76). – С. 139-147.
2. Моляков, А. С. Новый метод систематического поиска недекларированных возможностей ядра Windows NT 5.1 с введением контроля ContextHooking и PspCidHooking / А. С. Моляков // Вопросы защиты информации. – 2008. – № 1(80). – С. 49-56.
3. Моляков, А. С. Метод контроля отображения защищенных сегментов памяти при трансляции виртуальных адресов процессов ОС Windows / А. С. Моляков // Вопросы защиты информации. – 2008. – № 2(81). – С. 32-35.
4. Моляков, А. С. KPROCESSOR_CID_TABLE -факторинг – новое направление в теории компьютерного анализа вирусного кода и программных закладок / А. С. Моляков // Проблемы информационной безопасности. Компьютерные системы. – 2009. – № 1. – С. 7-18.
5. Моляков, А. С. KPROCESSOR-CID-table-факторинг в области создания защищенных ОС нового поколения / А. С. Моляков // Безопасность информационных технологий. – 2009. – Т. 16, № 4. – С. 125-129
6. Моляков, А. С. Модель скрытых угроз информационной безопасности в среде облачных вычислений / А. С. Моляков, В. С. Заборовский, А. А. Лукашин // Проблемы информационной безопасности. Компьютерные системы. – 2014. – № 2. – С. 41-46.
7. Моляков, А. С. Мультиграфовая модель операций для защиты среды облачных вычислений от скрытых угроз информационной безопасности / А. С. Моляков, В. С. Заборовский, А. А. Лукашин // Проблемы информационной безопасности. Компьютерные системы. – 2014. – № 2. – С. 37-40.
8. Моляков, А. С. Разработка прототипа вычислительного устройства с не фон-Неймановской архитектурой на базе отечественного микропроцессора стратегического назначения J7 / А. С. Моляков // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 1. – С. 22-28.
9. Моляков, А. С. Маркерное сканирование как новый научный подход в области создания защищенных информационных систем на примере ОС нового поколения Microtek / А. С. Моляков // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 1. – С. 29-36.

10. Моляков, А. С. Инновационный вариант развития защищенных супер-ЭВМ для решения важных задач фундаментальной медицины и инженерии в России / А. С. Моляков // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2022. – № 4-2. – С. 88-93. – DOI 10.37882/2223-2966.2022.04-2.26.

**В изданиях, индексируемых Scopus и Web of Science**

11. Molyakov, A. S. Model of hidden IT security threats in the cloud computing environment / A. S. Molyakov, V. S. Zaborovsky, A. A. Lukashin // Automatic Control and Computer Sciences. – 2015. – Vol. 49, No. 8. – P. 741-744. – DOI 10.3103/S0146411615080295.
12. Molyakov, A. S. Token scanning as a new scientific approach in the creation of protected systems: A new generation OS MICROTEK / A. S. Molyakov // Automatic Control and Computer Sciences. – 2016. – Vol. 50, No. 8. – P. 687-692. – DOI 10.3103/S0146411616080149.
13. Molyakov, A. S. A prototype computer with non-von Neumann architecture based on strategic domestic J7 microprocessor / A. S. Molyakov // Automatic Control and Computer Sciences. – 2016. – Vol. 50, No. 8. – P. 682-686. – DOI 10.3103/S0146411616080137.
14. Molyakov, A.S. New security descriptor computing algorithm of Supercomputers / A. Molyakov // Proceedings of the 3rd World Conference on Smart Trends in Systems, Security and Sustainability, WorldS4 2019. – 2019. – P. 349-350. – Art. No 8903965. – DOI 10.1109/WorldS4.2019.8903965.
15. Molyakov, A. S. Based on reconfiguring the supercomputers runtime environment new security methods / A. Molyakov // Advances in Science, Technology and Engineering Systems. – 2020. – Vol. 5, №3. – P. 291-298. – DOI 10.25046/aj050338.
16. Molyakov, A. S. Secured supercomputer technologies in Russia: functional computing units based on multithread-stream cores with specialized accelerators / A. S. Molyakov // Lecture Notes in Networks and Systems. – 2023. – Vol. 448. – P. 559-566. – DOI 10.1007/978-981-19-1610-6_49.

**В прочих изданиях**

17. Моляков, А. С. Обнаружение скрытых процессов в 3 кольце защиты ОС Windows / А. С. Моляков // Естественные и технические науки. – 2006. – № 6(26). – С. 257-264.
18. Моляков, А. С. Наиболее распространённые угрозы безопасности АС / А. С. Моляков // Естественные и технические науки. – 2006. – № 6(26). – С. 254-256.
19. Моляков, А. С. Новые методы поиска скрытых процессов ядра Windows NT 5.1 / А. С. Моляков // Программные продукты и системы. – 2007. – № 4. – С. 10.
20. Грушо, А. А. Исследование проектов верхнего и нижнего уровней политики безопасности ОС Windows / А. А. Грушо, А. С. Моляков // Программные продукты и системы. – 2007. – № 4. – С. 45-47.
21. Горбунов, В. Тихоокеанско-азиатские петафлопсы / В. Горбунов, П. Забеднов, А. Моляков // Открытые системы. СУБД. – 2011. – № 7. – С. 26.
22. Моляков, А. С. СуперЭВМ и операционные системы нового поколения / А. С. Моляков // Информационная безопасность: вчера, сегодня, завтра : сборник статей по материалам Международной научно-практической конференции, Москва, 23 апреля 2019 г. / Российский государственный гуманитарный университет, Институт информационных наук и технологий безопасности ; под редакцией В. В. Арутюнова. – Москва : Российский государственный гуманитарный университет, 2019. – С. 196-200.
23. Моляков, А. С. Модель угроз и теоретические основы метода реактивной защиты суперкомпьютеров / А. С. Моляков // Естественные и технические науки. – 2019. – № 7(133). – С. 197-201.
24. Моляков, А. С. Модель безопасных операций и метод реконфигурации среды выполнения программ суперкомпьютеров / А. С. Моляков // Естественные и технические науки. – 2019. – № 7(133). – С. 193-196.

25. Molyakov, A. Science Innovation Review: Developers of Supercomputers in Russia / A. Molyakov // Journal of Electrical and Electronic Engineering. – 2019. – Vol. 7, No. 5. – P. 107-112. – DOI 10.11648/j.jeee.20190705.12.

26. Molyakov, A. New-age Supercomputers: Hi-Speed Networks and Information Security / A. Molyakov // Journal of Electrical and Electronic Engineering. – 2019. – Vol. 7, No. 3. – P. 82-86. – DOI 10.11648/j.jeee.20190703.12.

27. Molyakov, A. S. Specialized hybrid Chinese microprocessors for solving important problems of fundamental medicine and national defense / A. S. Molyakov // Biomedical Journal of Scientific and Technical Research. – 2021. – Vol. 34, No. 4. – P. 26876-26881. – DOI 10.26717/BJSTR.2021.34.005573.

28. Molyakov, A. S. Revolutionary Direction of Secured Supercomputer Technologies Development in Russia / A. S. Molyakov // INFSEC 2021. Proceedings of the International Scientific and Practical Conference on Computer and Information Security, Yekaterinburg, Russian Federation, April 5-6, 2021. – Setúbal, Portugal: SciTePress, 2022. – P. 5-11. – DOI: 10.5220/0010616500003170.

29. Molyakov, A. S. Japanese Strategic Supercomputer "Arrow of Time" / A. S. Molyakov // Biomedical Journal of Scientific and Technical Research. – 2022. – Vol. 45, No. 2. – P. 36348-36351. – DOI 10.26717/BJSTR.2022.45.007183.

30. Molyakov, A. Mathematical Modeling of Neurodynamic Systems: Solving DIS-Tasks Using Massive-Multithread Supercomputers / A. Molyakov // Biomedical Journal of Scientific and Technical Research. – 2019. – Vol. 21, No. 5. – P. 16159-16162. – DOI 10.26717/BJSTR.2019.21.003657.

31. Molyakov, A. S. New Multilevel Architecture of Secured Supercomputers / A. S. Molyakov // Current Trends in Computer Sciences & Applications. – 2019. – Vol. 1, No. 3. – P. 57-59. – DOI 10.32474/CTCSA.2019.01.000112.

**Патенты РФ на изобретения**

32. Патент № 2618367 C1 Российская Федерация, МПК G06F 12/02. Вычислительное устройство программно-аппаратного комплекса : № 2016110564 : заявл. 23.03.2016 : опубл. 03.05.2017, Бюл. 13 / А. С. Моляков ; правообладатель Моляков А.С. – 2 с. : ил.

33. Патент № 2626350 C1 Российская Федерация, МПК G06F 12/02. Способ функционирования операционной системы вычислительного устройства программно-аппаратного комплекса : № 2016113545 : заявл. 11.04.2016 : опубл. 26.07.2017, Бюл. 21 / А. С. Моляков ; правообладатель Моляков А.С. – 2 с. : ил.

**Свидетельства о государственной регистрации программ для ЭВМ**

34. Свидетельство о государственной регистрации программы для ЭВМ № 2014616744. Альфа-монитор : № 2014613359 : заявл. 15.04.2014 / А. С. Моляков ; правообладатель Моляков А. С.