МИНИСТЕРСТВО ОБОРОНЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБОРОНЫ РОССИИ)
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
4 ЦЕНТРАЛЬНЫЙ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
ИНСТИТУТ
МИНИСТЕРСТВА ОБОРОНЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ул. Тих[illegible], 22, Мытищи, мкр., 141091

«___»_____20___г. №_____

На №_____

Экз. № 1

УТВЕРЖДАЮ
Заместитель начальника 4 Центрального научно-исследовательского института Министерства обороны Российской Федерации по научной работе

В. Шкарбань

«_4_» марта 2024 года.

ОТЗЫВ

4 ЦНИИ Минобороны России

на автореферат диссертации Молякова Андрея Сергеевича на тему: «Модели и методы обеспечения информационной безопасности стационарных и бортовых суперкомпьютерных вычислительных систем», представленную на соискание ученой степени доктора технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Актуальность исследований. В настоящее время в Российской Федерации различными предприятиями ведутся работы по созданию и поставкам вычислительных систем кластерного типа высокой производительности, основу которых составляют коммерчески доступные компоненты и сборочные единицы зарубежного производства. Большинство элементов компонентной элементной базы, используемых для создания супер-ЭВМ (суперкомпьютеров), зарубежного производства. Это приводит к появлению недоверенных элементов в сборке, импортируемых из-за рубежа. Ядро операционных систем и основные модули общего программного обеспечения для суперкомпьютеров, как правило, зарубежного производства или в них используется свободно распространяемый открытый программный код.

Факты обнаружения вредоносного кода в аппаратно-программных средствах России и других стран широко известны. При проведении пусконаладочных работ, изменении конфигурации, обновлении и установке дополнительных программных и технических средств высокая вероятность внедрения вредоносных программ в суперкомпьютеры локально или по сети. В результате выполнения непреднамеренных или преднамеренных действий

нарушителя или штатного обслуживающего персонала также высока вероятность нарушения функционировании, что недопустимо для современных суперкомпьютеров при выполнении сложных инженерно-расчетных высоконагруженных информационных задач.

В представленной соискателем работе рассмотрены два типа суперкомпьютеров: бортовые (например, «Грифон» или «Комдив») и стационарные («Ангара» ЕС1740, СТ-2, Tsubame 3.0).

Для стационарных суперкомпьютеров в зависимости от набора конфигураций заданы три профиля защиты: малого промышленного кластера - уровень защиты средний, суперкластера крупного технологического объекта - уровень защиты высокий, масштабных информационно-аналитических центров - уровень защиты максимальный. По сравнению со стационарными суперкомпьютерами бортовые супер-ЭВМ обладают ограниченными вычислительными ресурсами, набор функций безопасности и режимов защиты для них базовый (минимальный).

Обрабатываемая с использованием суперкомпьютеров информация обычно связана с решением вопросов национальных проектов, моделирования систем энергетики, транспорта, решением ресурсоемких научно-технических и промышленных задач, а также с управлением объектами критической информационной инфраструктуры.

Наличие потенциальных уязвимостей в суперкомпьютерах с недоверенными зарубежными аппаратно-программными модулями обуславливают возможность реализации на них неизвестных компьютерных атак нарушителя со значительным материальным ущербом.

В настоящее время перспективные системы информационной безопасности суперкомпьютеров разрабатываются с использованием технологии виртуализации. Ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты осуществляется за счёт реконфигурации элементов и их восстановления после воздействий компьютерных атак.

Таким образом, проведенные Моляковым А.С. исследования, направленные на разработку моделей и методов обеспечения информационной безопасности стационарных и бортовых суперкомпьютерных вычислительных систем, являются **актуальными** и представляют несомненный практический интерес.

Научная задача диссертации заключается в разработке моделей и методов обеспечения информационной безопасности стационарных и

бортовых суперкомпьютерных вычислительных систем.

Целью диссертационной работы является обеспечение информационной безопасности суперкомпьютеров на основе разработки моделей и методов гибридной защиты информации за счет использования гипервизоров и реконфигурации структуры суперкомпьютеров в условиях недоверенной вычислительной среды и компьютерных атак нарушителя.

Объектом исследования являются системы информационной безопасности стационарных и бортовых суперкомпьютерных вычислительных систем.

Предметом исследования являются модели и методы обеспечения информационной безопасности суперкомпьютерных вычислительных систем с применением средств виртуализации.

Научными результатами, выносимыми на защиту, являются:

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.

Научная новизна полученных в ходе диссертационных исследований результатов заключается в разработке:

теоретических и научно-методических принципов защиты суперкомпьютеров с использованием средств виртуализации, основанных на построении и формализации универсальных и равномерных функций оценки безопасных состояний СК для заданных классов операций, отличающихся нахождением в n-мерной алгебраической системе инварианта и позволяющих решить научную проблему супервентности для отрасли промышленности;

модели угроз целостности среды выполнения процессов, основанной на новой парадигме написания правил политики безопасности, отличающейся заданием сущностей вместо классической связки «субъект, объект, предикат» - «субъект», «объект» и «дескриптор оценки безопасности состояний» и позволяющей описать и формализовать каждую i-ую угрозу аргументов в виде конъюнкции предикатов из восьми логических переменных;

модели безопасных операций, основанной на декомпозиции информационных процессов в виде 8-уровневой иерархической структуры и принципах кибериммунитета, отличающейся 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 и позволяющей идентифицировать и блокировать разные классы уязвимостей на всех уровнях иерархии выполнения запросов, что подтверждается сформулированным условием разрешимости и доказанной теоремой;

метода реактивной защиты суперкомпьютеров, основанного на виртуализации среды выполнения процессов, если вычисленный дескриптор состояния попадает в зону «риска», отличающегося применением траекторий вычислений дескрипторов оценки безопасности состояний на структурах Крипке и позволяющего создать единую технологию выявления уязвимостей и реализовать полный контроль контекста и тайминга выполняемых операций на недоверенной аппаратуре;

метода реконфигурации среды выполнения проактивной защиты суперкомпьютеров, основанного на парадигме темпоральной логики для проверки истинности принимаемых решений на структурах Крипке, отличающегося вычислением доверительной вероятности в качестве показателя защищенности компонентов среды на наборах тегированных данных в виде согласованной вариации факторных и результативных признаков и позволяющего на ранней стадии обнаруживать новые классы уязвимостей и противодействовать им путем автоматической реконфигурации структуры;

методики тестирования уровня защищенности, основанной на алгоритме “маркерного” сканирования, отличающейся использованием набора меток: сочетаниям меток сопоставляются признаки скрытых угроз и действия, отвечающие требованиям выбранной политики информационной безопасности и позволяющей повысить уровень защищенности вычислительных ресурсов СК и минимизировать ошибки 1-го и 2-го рода.

программно-технических решений, основанных на разработанных моделях и методах, отличающихся 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) и позволяющим реализовать гарантированно защищенные системы, адаптированные к потоку входных данных и наборам конфигураций вычислительной среды.

Практическая значимость диссертационных исследований заключается в том, что:

разработаны технологии и программно-технические средства на основе предложенных моделей и методов, составляющих принципы реактивной и проактивной защиты информации в суперкомпьютерах;

предложено 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;

предложены технологические решения, которые в нескольких вариантах позволяют снизить затраты на производство суперкомпьютеров за счёт переноса большей части испытаний с опытных образцов на программное обеспечение.

Теоретическая значимость полученных результатов состоит в том, что разработанные и предложенные модели и методы, составляют теоретическую основу информационной безопасности суперкомпьютеров на основе реактивной и проактивной защиты информации, реконфигурации элементов суперкомпьютеров при недоверенной вычислительной среде и компьютерных атаках.

Достоверность и обоснованность результатов достигнута корректным применением методов исследований и подтверждается результатами их практического использования, адекватностью представления исследуемых процессов в суперкомпьютерах, а также апробацией результатов исследования в ходе вычислительных экспериментов.

Научные результаты исследования были реализованы и внедрены:

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;

в рамках китайского проекта по разработке защищенных суперкомпьютерных вычислительных комплексов серии Tian-he/CT-2;

в рамках японского проекта по созданию суперкомпьютера с высокими показателями производительности и защищенности серии Tsubame 3.0;

в учебном процессе и научных исследованиях на кафедре «Комплексная защита информации» ФГБОУ ВО «РГГУ».

Структура и объём автореферата. Автореферат достаточно полно отражает содержание и научные результаты, представленные в нем. Оформление автореферата соответствует требованиям ГОСТ 7.0.11-2011 «Диссертация и автореферат диссертации. Структура и правила оформления». Автореферат соответствует требованиям Положения о порядке присуждения ученых степеней Минобнауки России. Тема исследования соответствует паспорту специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Однако следует отметить следующие **недостатки диссертации.**

1. В автореферате отсутствует математическая постановка научной проблемы, выбранный интегральный показатель и методическая схема исследований, что затрудняет представление о систематизации предлагаемых автором методов и моделей для достижения цели обеспечения информационной безопасности стационарных и бортовых суперкомпьютерных систем.

2. В модели угроз целостности среды выполнения процессов не представлены рассмотренные уязвимости и возможности средств нарушителя по реализации угроз нарушения информационной безопасности стационарных и бортовых суперкомпьютерных систем.

3. В методике тестирования уровня защищенности суперкомпьютеров четко не обоснован требуемый объем тестирования и количество тестов на проникновение для проверки реального уровня информационной безопасности суперкомпьютеров при компьютерных атаках нарушителя.

4. В методе реконфигурации среды выполнения проактивной защиты суперкомпьютеров не описаны возможные компьютерные инциденты и порядок реагирования на них при обеспечении необходимого уровня устойчивости функционирования исследованных суперкомпьютеров к компьютерным атакам.

Отмеченные недостатки **не снижают** общую положительную оценку полученных автором научных результатов и их практическую значимость.

Выводы. Содержание автореферата позволяет считать, что диссертация Молякова А.С. является завершённой научно-квалификационной работой, выполненной лично автором, в которой решена актуальная научная задача. Все результаты, представленные в диссертационной работе, получены лично автором в процессе выполнения научно-исследовательских и опытно--конструкторских работ. По степени новизны, своей научной значимости и практической ценности работа удовлетворяет требованиям п. 9 Постановления Правительства Российской Федерации от 24 сентября 2013 г. № 842 «Положение о присуждении ученых степеней», предъявляемым к докторским диссертациям, а ее автор, Моляков Андрей Сергеевич заслуживает присуждения ему ученой степени доктора технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Отзыв обсужден и одобрен на заседании научно-технического совета научно-исследовательского управления 4 ЦНИИ Минобороны России 4 марта 2024 года, протокол № 8/24.

Отзыв подготовил старший научный сотрудник научно-исследовательского отдела, кандидат технических наук

С.В. Купин

« 4 » марта 2024 г.

Главный научный сотрудник научно-исследовательского управления, доктор технических наук, профессор

С.М. Климов

« 4 » марта 2024 г.

Начальник научно-исследовательского отдела, кандидат технических наук

С.Г. Антонов

« 4 » марта 2024 г.

141091, г. Королев, Московская обл., ул. Тихонравова, д. 29

Авторы отзыва:
Купин Сергей Владимирович,
Климов Сергей Михайлович