ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертационную работу Молякова Андрея Сергеевича «Модели и методы обеспечения информационной безопасности стационарных и бортовых суперкомпьютерных вычислительных систем», представленную на соискание ученой степени доктора технических наук по научной специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность», технические науки

1. Актуальность темы диссертационного исследования

В диссертационной работе Молякова А.С. рассмотрены стационарные и бортовые суперкомпьютерные вычислительные системы. Переходя на уровень инженерных решений для суперкомпьютеров (СК), производители оборудования реализовали для системных разработчиков встроенную полнофункциональную поддержку технологии виртуализации для разного набора микропроцессоров и микроконтроллеров. Других штатных функций безопасности у аппаратных модулей и сборочных конструктивов, из которых собираются компоненты суперкомпьютеров, просто нет. С использованием технологии виртуализации можно реализовать многоуровневый контроль всех взаимодействий между доменами безопасности.

Из всего выше сказанного можно сделать вывод о том, что в современных условиях средства защиты информации суперкомпьютеров разрабатываются с использованием виртуализации оборудования, поскольку она позволяет повысить гибкость использования и функционирования оборудования, обеспечивая этим совместное функционирование разных операционных систем, поддержку ЭВМ с разной архитектурой сборки, оптимизировать развиваемую производительность и энергоэффективность.

Перечисленные особенности определяют актуальность научной проблемы в области создания защищенных стационарных и бортовых суперкомпьютерных систем.

2. Личный вклад автора

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». Личный вклад автора в теорию:

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.

3. Оценка достоверности и новизны полученных результатов

Автором проведены теоретические и практические исследования и получены научные результаты, которые подтверждаются соответствующими актами внедрения, 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 новизна работы состоит в следующем:

1. Разработаны теоретические и научно-методические принципы защиты суперкомпьютеров с использованием средств виртуализации, отличающиеся нахождением в n-мерной алгебраической системе инварианта.
2. Разработана модель угроз целостности среды выполнения процессов, основанная на новой парадигме написания правил политики безопасности, 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.

4. Разработан и исследован метод реактивной защиты суперкомпьютеров, основанный на виртуализации среды выполнения процессов, 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.

6. Разработана методика тестирования уровня защищенности, основанная на алгоритме "маркерного" сканирования.

7. Разработаны программно-технические решения, основанные на разработанных моделях и методах, отличающиеся минимальными затратами ресурсов для создания обучающих кластерных зон и на обучение.

В диссертационном исследовании соискателем решена важная **научная проблема** супервентности для отрасли промышленности, связанной с проектированием и внедрением средств защиты информации для суперкомпьютеров в стационарном и бортовом исполнении.

4. Оценка содержания диссертации

Диссертация состоит из введения, пяти глав, заключения и четырех приложений.

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 суперкомпьютеров.

Во второй главе введены новые теоретические и научно-методические принципы защиты суперкомпьютеров с использованием средств виртуализации, решена научная проблема супервентности. Правила политик безопасности задаются в виде модальных конструкций в терминах темпоральной логики. 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. Система динамически эволюционирует и модифицирует наборы модальных правил на основе грамматик темпоральной логики 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.

В четвертой главе разработаны метод реактивной защиты и метод реконфигурации среды выполнения программ проактивной защиты на основе применения маркеров и интервально-временных ограничений.

В пятой главе приведена реализация авторского программно-технического решения «Альфа-монитор», состоящего из проксирующих модулей и модуля верификации команд гипервизора, программных агентов сбора метрики приложений и мониторинга событий безопасности.

В Заключении сформулированы основные теоретические и практические результаты исследований.

5. Соответствие паспорту специальности

Выполненное соискателем исследование соответствует п. 3 «Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса» и п. 15 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию

существующих средств защиты информации и обеспечения информационной безопасности определения специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

6. Замечания по диссертационной работе

При изучении диссертации отмечены следующие недостатки:

1. В диссертации п.3 паспорта специальности записан некорректно (стр 14).

2. Подсистема обеспечения информационной безопасности для отечественных и зарубежных суперкомпьютерных вычислительных платформ реализована для защиты от несанкционированного доступа на базе технологических модулей «Альфа-монитор». Представлено техническое описание разработанных моделей и методов, программного обеспечения, конструктива сборок экспериментальных образцов и серийно выпускаемой продукции для китайских и японских супер-ЭВМ. В части российских разработок защищенных отечественных стационарных суперкомпьютерных систем упоминаются только решения для суперкомпьютерных комплексов серии «Ангара» ЕС1740. Однако в работе уделено мало внимания альтернативным российским суперкомпьютерным платформам, например, «Эльбрус» 8С/16С, «Байкал» Т1/Т2. Хотя в Главе 5 представленной диссертации автор указывает, что инициативной группой разработчиков реализована поддержка вычислительных модулей на базе «Эльбрус», «Байкал», но сейчас пока ведутся совместные работы с целевыми заказчиками по наладке и тестированию оборудования.

3. При описании методики тестирования и алгоритма “маркерного” сканирования автором достаточно хорошо и информативно проиллюстрированы разработанные принципы и подходы, однако местами изложение фрагментарное, не освещены подробно инженерные решения при работе с бортовыми супер-ЭВМ и крупными промышленными кластерами, например, широко используемые высокопроизводительные вычислительные модули серии «Багет Р2А», которые устанавливаются в вычислительную и коммуникационную технику, в качестве управляющего процессора в

контроллерах, станках, на летательных и космических аппаратах, а также другом специальном оборудовании.

4. Полагаю, что указанные выше недостатки обусловлены тем, что исследования и проверки по требованиям ФСТЭК России в части изучения дестабилизирующих воздействий на специализированые СБИС «Комдив» 1890ВМ8Я, 1890ВМ5Ф, 1907ВМ028, 1907ВМ028 для стационарных суперкомпьютерных комплексов, СБИС «Комдив» 5890ВМ1Т, 1900ВМ2Т 1907ВМ044, 1890ВМ6Я 1890ВМ7Я – для бортовых супер-ЭВМ, используемых в национальных суперкомпьютерных системах, имеют закрытый характер. Поэтому в тексте диссертации представлена только открытая часть защиты суперкомпьютеров от средств скрытого информационного воздействия.

5. В Заключении на стр. 259 и стр. 260 целесообразно было бы указать в качестве дальнейших перспектив разработки реализацию подсистемы обеспечения информационной безопасности для мобильных платформ крупных телекоммуникационных провайдеров. Сейчас это направление является очень востребованным в рамках создания национальных распределенных информационных систем.

Однако указанные замечания не влияют на общую положительную оценку работы и не снижают вклад автора в решение важной научной задачи.

Заключение

Несмотря на изложенные выше замечания, диссертационную работу Молякова А.С. «Модели и методы обеспечения информационной безопасности стационарных и бортовых суперкомпьютерных вычислительных систем» следует признать законченной научно-квалификационной работой, выполненной на актуальную тему.

Поддержание максимального уровня гарантированной защищенности суперкомпьютеров реализовано на основе разработки моделей и методов гибридной (реактивной и проактивной) защиты за счет использования гипервизоров, обеспечивающих надёжную защиту от угроз информационной безопасности.

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

Диссертация соответствует требованиям, установленным Положением «О присуждении ученых степеней в федеральном государственном автономном образовательном учреждении высшего образования «Южный федеральный университет». Моляков Андрей Сергеевич заслуживает присуждения ученой степени доктора технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность», технические науки.

Официальный оппонент:

Лепешкин Олег Михайлович

доктор технических наук (специальность 05.13.10 – «Управление в социальных и экономических системах»), доцент, доцент кафедры безопасности инфокоммуникационных систем специального назначения, Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи имени маршала Советского Союза С.М. Буденного»

194064, г. Санкт-Петербург, К-64, Тихорецкий проспект, д.3

Тел.: 8 (812) 247-98-35

E-mail: lepechkin1@yandex.ru

доктор технических наук, доцент О.М. Лепешкин

«12» 02 2024 г.

Подпись Лепешкина О.М. заверяю:

М.П.

ПОМОЩНИК НАЧАЛЬНИКА ВАС по СВиБВС
НАЧАЛЬНИК СТРОЕВОГО ОТДЕЛА
ПОДПОЛКОВНИК А. Головин

« » 202 г.