DOI 10.37882/2223-2966.2025.04.29

НАУЧНО-ТЕХНОЛОГИЧЕСКИЕ РЕШЕНИЕ ПО ОБЕСПЕЧЕНИЮ ГИБРИДНОЙ ЗАЩИТЫ СОВРЕМЕННЫХ СУПЕРКОМПЬЮТЕРОВ В УСЛОВИЯХ СЕТЕЦЕНТРИЧЕСКИХ КИБЕРВОЙН

SCIENTIFIC AND TECHNOLOGICAL SOLUTIONS FOR PROVIDING HYBRID PROTECTION OF MODERN SUPERCOMPUTERS IN THE CONDITIONS OF NETWORK-CENTRIC CYBERWARS

A. Molyakov

Summary. The article describes the subsystem for ensuring information security of the «Angara» EC1740 series supercomputers developed by the author, implemented based on the «Alfa-Monitor» multi-domain hypervisor and «Angara-MVS» switches with the implementation of hybrid protection methods. The scientific and technological solution is based on the reactive protection method and the method of reconfiguring the proactive protection environment, which allow detecting any types of computer attacks at all levels of the request execution hierarchy and counteracting them by automatically reconfiguring the configuration structure of the executable environment.

Keywords: «Angara» EC1740, secure multi-domain hypervisor, hybrid protection.

Моляков Андрей Сергеевич
Кандидат технических наук, доцент, Российский государственный гуманитарный университет, г. Москва
andrei_molyakov@mail.ru

Аннотация. В статье описывается разработанная автором подсистема обеспечения информационной безопасности суперкомпьютеров серии «Ангара» ЕС1740, реализованная на базе мультидоменного гипервизора «Альфа-монитор» и коммутаторов «Ангара-МВС» с реализацией методов гибридной защиты. Научно-технологическое решение основано на методе реактивной защиты и методе 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.

Ключевые слова: «Ангара» ЕС1740, защищенный мультидоменный гипервизор, гибридная защита.

Введение

В современных условиях стационарные и бортовые суперкомпьютеры играют ключевую роль в решении важнейших военных задач, включая автоматизированное управление системами вооружения, координацию разведывательно-ударных групп, а также создание автономных боевых роботов. Эти разработки напрямую связаны с концепциями войн шестого поколения.

При создании стационарных и бортовых суперкомпьютеров сегодня невозможно обойтись без виртуализации их аппаратной части. Такой подход повышает гибкость использования оборудования, позволяя одновременно работать с различными операционными системами (ОС) в рамках сложных аппаратно-программных комплексов.

Это также способствует улучшению производительности и энергоэффективности, а также предоставляет возможность реконфигурации, что важно не только для восстановления после сбоев, но и для защиты от кибератак и других специальных воздействий.

Виртуализация аппаратной части суперкомпьютеров также открывает новые возможности для интеграции искусственного интеллекта (ИИ) в военные системы. Это позволяет создавать адаптивные алгоритмы, способные анализировать большие объемы данных в реальном времени, прогнозировать действия противника и принимать решения с минимальным вмешательством человека. Такие системы могут быть использованы для управления беспилотными летательными аппаратами, автоматизации логистики и даже для разработки стратегий ведения боевых действий.

Кроме того, виртуализация способствует повышению уровня кибербезопасности. Возможность быстрой реконфигурации систем позволяет оперативно реагировать на угрозы, минимизируя уязвимости. Это особенно важно в условиях, когда противник использует сложные методы кибератак, включая внедрение вредоносного программного обеспечения (ПО).

1. Недостатки современных технологий защиты информации в высокопроизводительных вычислительных комплексах

Современные программно-технические решения, внедренные в оборонно-промышленный комплекс Рос-

сии, ориентированы на классические вычислительные кластеры, не учитывая инновационные суперкомпьютерные технологии, такие как многоядерность, высокопараллельность, асинхронность обработки данных, сложные иерархические сети и др. Без этих элементов невозможно эффективно противостоять внешним угрозам и выявлять новые риски на всех уровнях архитектуры суперкомпьютеров.

Использование гибридных вычислителей с гибкой настройкой окружения, мультитредовой архитектурой для сбора метрик и защищенных мультидоменных гипервизоров, а также внедрение специализированных внутрикристальных и межмодульных сетей позволяют не только преодолеть отставание в производительности, но и опередить потенциальных противников в сетецентрических войнах.

Современные системы защиты высокопроизводительных вычислительных комплексов имеют ряд недостатков. Во-первых, сложность элементной базы увеличивает риск внедрения вредоносных компонентов. Во-вторых, высококвалифицированные пользователи повышают вероятность внутренних атак. В-третьих, атаки часто поддерживаются государственными структурами (например, иностранными спецслужбами). В-четвертых, злоумышленники могут быстро анализировать уязвимости и проводить масштабные атаки.

Особую угрозу представляет использование импортных компонентов, таких как GPU-ускорители, которые могут быть источником внутренних рисков. Ни физическая изоляция, ни отключение от сетей не гарантируют безопасность, так как угрозы заложены в самой архитектуре.

Для минимизации рисков необходимо внедрение отечественных решений, основанных на принципах доверенной элементной базы и аппаратной верификации. Разработка специализированных процессоров с поддержкой многоядерности и асинхронных вычислений, а также создание защищенных межмодульных сетей с динамической маршрутизацией позволят снизить зависимость от импортных технологий. Важным шагом является интеграция систем мониторинга на уровне аппаратного обеспечения, способных выявлять аномалии в режиме реального времени.

Ключевым элементом защиты становится использование мультидоменных гипервизоров, обеспечивающих изоляцию критически важных процессов и данных. Такие системы должны поддерживать гибкую настройку окружения, адаптируясь к изменяющимся угрозам.

Использование специализированных внутрикристальных сетей с поддержкой сложных иерархий и высокопараллельных вычислений позволит повысить производительность и устойчивость к атакам.

Для противодействия внутренним угрозам необходимо также внедрение систем контроля доступа на основе поведенческого анализа и машинного обучения. Это позволит выявлять аномалии в действиях пользователей и предотвращать утечки данных. Одновременно требуется развитие технологий защиты от атак, эксплуатирующих уязвимости в архитектуре импортных компонентов, включая GPU-ускорители.

2. Новые задачи обеспечения информационной безопасности в связи с появлением суперкомпьютеров

Для обеспечения безопасности суперкомпьютеров требуется внедрение многоуровневой защиты, включающей комплексный контроль их функционирования. Обработка значительных объемов данных, поступающих от таких систем мониторинга, требует применения специализированных аппаратно-программных решений.

Для решения подобных задач создаются массово-мультитредовые суперкомпьютеры, где проблема длительных задержек при доступе к памяти устраняется за счет оптимизации работы приложений и оборудования. Это позволяет достичь высокой пропускной способности памяти, создавая эффект минимальных задержек при выполнении операций. Например, в США, Японии и Китае активно разрабатываются такие системы и их компонентная база.

Основная угроза для российских суперкомпьютеров связана с использованием импортных компонентов, таких как высокоскоростные микропроцессоры и ускорители. Важно исследовать возможные аппаратные закладки, методы их выявления и устранения.

Необходимо возродить отечественные разработки в области элементной базы и архитектуры суперкомпьютеров, устойчивых к атакам, сбоям и отказам. Для минимизации рисков, связанных с использованием импортных компонентов, нужно развивать отечественные технологии производства процессоров, памяти и других критически важных элементов. Это требует значительных инвестиций в научные исследования, разработку новых архитектур и создание производственных мощностей.

Особое внимание следует уделить созданию систем, устойчивых к кибератакам, включая защиту от аппаратных закладок и программных уязвимостей. Важным шагом станет интеграция отечественных суперкомпьютеров в глобальные исследовательские проекты, что позволит не только повысить их конкурентоспособность,

но и обеспечить обмен опытом с ведущими мировыми разработчиками.

При этом необходимо учитывать современные тенденции, такие как использование квантовых вычислений и нейроморфных архитектур, которые могут стать основой для следующего поколения суперкомпьютеров.

Для успешной реализации таких проектов требуется тесное взаимодействие между государством, научными институтами и частным сектором. Только комплексный подход к созданию и защите суперкомпьютеров позволит России сохранить технологический суверенитет и конкурировать на мировом уровне.

Необходимо модернизировать образовательные программы, внедряя в них современные подходы к изучению микроэлектроники, квантовых технологий и кибербезопасности. Создание специализированных центров компетенций и лабораторий позволит студентам и молодым ученым работать с передовым оборудованием и участвовать в инновационных проектах.

Кроме того, важно стимулировать экспорт отечественных решений в области суперкомпьютеров и микроэлектроники. Это не только укрепит экономику, но и повысит доверие к российским технологиям на международной арене в рамках БРИКС и др.

3. Подсистема обеспечения информационной безопасности современных суперкомпьютеров на базе технологических модулей «Альфа-монитор»

Гибридная защита суперкомпьютеров предполагает интеграцию различных методов и технологий для обеспечения комплексной безопасности. Одним из ключевых подходов является сочетание аппаратных и программных решений.

Аппаратные методы включают использование специализированных модулей безопасности, таких как криптографические процессоры, которые обеспечивают защиту данных на физическом уровне.

Программные методы, в свою очередь, охватывают системы мониторинга, анализа угроз и управления доступом, что позволяет оперативно выявлять и нейтрализовать компьютерные атаки.

Кроме того, гибридная защита включает использование проактивной и реактивной защиты, многофакторной аутентификации и распределенных систем хранения данных. Это позволяет минимизировать риски утечки информации и обеспечить отказоустойчивость системы. Таким образом, гибридная защита суперкомпьютеров представляет собой многоуровневую систему, которая сочетает передовые технологии для обеспечения максимальной безопасности и устойчивости к кибератакам.

Метод реконфигурации среды выполнения программ проактивной защиты суперкомпьютерных комплексов с учетом мобильности позволяет формировать изолированную среду исполнения для различных типов суперкомпьютеров с гибкой настройкой окружения и контекста вызовов сервисов, а также сбором метрик приложений [1]. Это применимо не только для коммерческих зарубежных процессоров, но и для отечественных специализированных СБИС, таких как «КОМДИВ», «Байкал», «Эльбрус» и др.

Метод реактивной защиты, основанный на виртуализации среды выполнения, использует траектории вычислений для оценки безопасности состояний на структурах Крипке. Это позволяет разработать типовую технологию выявления уязвимостей и контролировать контекст и тайминг операций на недоверенном оборудовании [2].

На основе модели безопасных операций реализованы функции оценки состояния системы через «свертку» атрибутов процессов и конфигурации среды с заданной масштабируемостью, а с учетом модели угроз разработана технология следящих действий со стороны гипервизора и контроллеров транзакционной памяти [3, 4]. Показатели защиты адаптированы к задачам и требованиям передачи данных между мобильными (бортовыми) и стационарными суперкомпьютерными вычислительными системами.

Нами разработан многокомпонентный защищенный гипервизор, включающий проксирующие модули, верификатор команд и монитор безопасности [5, 6]. Подсистема безопасности суперкомпьютеров «Ангара» ЕС1740 использует гипервизор «Альфа-монитор» и коммутаторы «Ангара-МВС», поддерживая как зарубежные, так и отечественные защищенные ОС.

Гипервизор «Альфа-монитор» в связке с контроллерами аппаратной транзакционной памяти обеспечивает изоляцию вычислительных процессов, что позволяет минимизировать риски утечек данных и несанкционированного доступа. Он поддерживает динамическую адаптацию конфигурации среды выполнения в зависимости от текущих угроз и требований задач, а также механизмы автоматического восстановления после сбоев, что обеспечивает непрерывность выполнения критически важных задач. Для этого используются алгоритмы анализа траекторий вычислений, которые интегрированы в модуль верификации команд [7]. В случае обнаружения аномалий система переключается на резервные модули, сохраняя работоспособность без потери данных.

Интеграция с системами мониторинга и управления безопасностью позволяет оперативно реагировать на изменения в угрозах. Это особенно важно для работы в условиях высоконагруженных сред, где требуется минимизация задержек при обработке данных. Реализована также масштабируемость, что позволяет адаптировать систему под растущие нагрузки без снижения производительности [8]. Благодаря модульной архитектуре пользователи могут гибко настраивать функционал под конкретные задачи, добавляя или удаляя компоненты по мере необходимости. Это делает решение подходящим как для небольших проектов, так и для крупных корпоративных инфраструктур.

Важной его особенностью является поддержка виртуализации на уровне оборудования, что значительно повышает эффективность использования ресурсов. Это позволяет снизить затраты на обслуживание и энергопотребление, сохраняя при этом высокий уровень производительности. Также поддерживается миграция виртуальных машин между узлами без прерывания работы, что особенно важно для обеспечения отказоустойчивости.

Монитор безопасности гипервизора обеспечивает контроль за передачей данных между мобильными (бортовыми) и стационарными высокопроизводительными системами, включая проверку целостности и конфиденциальности информации.

Поддержка гибридных сред выполнения позволяет интегрировать решение в информационные системы с различными типами ОС, включая специализированные версии для суперкомпьютеров.

Заключение

Подводя итог проведенных теоретических и практических исследований, можно отметить следующее: нами разработано и реализовано научно-технологическое решение для экономики и техники РФ — это создание доверенной среды вычислений для национальных суперкомпьютерных платформ «Ангара» серии ЕС1740. Хотелось бы отметить, что допущения и предположения, основанные на разбиении системы на изолированные домены безопасности, интеграции с аппаратной транзакционной памятью и введении многоуровневого контроля взаимодействий, делающие недоверенную среду функционирования защищенной, подтверждены результатами стендовых испытаний.

В планах на будущее внедрить решение по гибридной защите для российского суперкомпьютера класса «Арктур», который содержит 16 вычислительных модулей по шесть ПЛИС XCVU37P Xilinx семейства UltraScale+ в каждом.

В части разработки и реализации перспективных национальных информационных систем с использованием суперкомпьютерных технологий в условиях сетецентрических войн сформулируем основные выводы:

1) Новые модели угроз целостности среды исполнения и модель безопасных операций позволяют создавать защищенные суперкомпьютерные комплексы с повышенными характеристиками сбоеустойчивости к внешним специальным воздействиям и новым классам компьютерных атак.
2) Новые авторские методы гибридной (реактивной и проактивной) защиты учитывают специфику суперкомпьютеров в целом (высокая производительность, высокопараллельные и асинхронные процессы, огромной поток данных и т.д.).
3) Запатентованная автором технология следящих действий со стороны гипервизора и контроллеров транзакционной памяти не допускает аварийного завершения работы ответственных приложений.
4) Учтены механизмы контроля работоспособности доступной кэш-памяти низкоуровневыми модулями гипервизора и контролеров памяти в процессе работы процессора на примере отечественных специализированных СБИС.
5) Если сейчас не учесть поддержку дальнейшего развития принципиально новых, прорывных проектно-конструкторских решений и их промышленного внедрения, отставание российской промышленности в части создания защищенных суперкомпьютерных комплексов Петафлопсного и более уровня производительности в дальнейшем уже не получится компенсировать.

ЛИТЕРАТУРА

1. 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
2. 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.
3. 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.
4. 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.

5. 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. 9.
6. 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
7. 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.
8. 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.