г. Таганрог, ул. Шевченко 2, «Точка кипения» Инженерно-технологической академии Южного федерального университета, Диссертационный совет ЮФУ 801.02.02
Ельчаниновой Н.Б.

ОТЗЫВ

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

Интенсивное развитие высокопроизводительных вычислительных платформ (суперкомпьютеров) поставило ряд проблем, связанных с проектированием архитектуры их информационной безопасности и разработкой методов и технологий ее обеспечения. Высокая производительность суперкомпьютеров, достигающие несколько петафлопсов, огромные ресурсы памяти и многозадачный режим, с различным уровнем доступа и конфиденциальности информации в значительной степени меняют структуру модели угроз, в которых целями кибератак являются не только хранимые данные, но и возможность получения доступа к вычислительным ресурсам мощнейших компьютеров. Отсюда возникает проблема доверия к процессам и результатам вычислений на суперкомпьютерах. Существующие подходы к созданию оценочных уровней доверия на основе стандартов 15408 вряд ли возможны, поэтому требуются новые подходы к решению этой сложной задачи. Это и определяет актуальность работы.

Цель работы сформулирована как «получение и поддержание максимального уровня гарантированной защищенности суперкомпьютеров на основе моделей и методов гибридной защиты за счёт использования гипервизоров, обеспечивающих надёжную защиту от угроз информационной безопасности реализуемых с использованием средств скрытого информационного воздействия». Считаю, что цель достигнута.

В автореферате отражены следующие научные результаты.

1. Разработаны теоретические и научно-методические принципы защиты суперкомпьютера с использованием средств виртуализацией, основанный на построении и формализации оценок безопасных состояний суперкомпьютера в форме дескрипторов оценок безопасности состояния системы, которые вычисляется на основе атрибутов протекающих процессов. Такой подход является новым, так как позволяет выявить аномалии в процессах обработки данных и соотнести их с конкретными угрозами.
2. Разработана модель безопасных операций, позволяющие идентифицировать и блокировать разные классы уязвимости на всех уровнях иерархии выполнения запросов. Это подтверждается сформулированным условиям разрешимости и доказанный теоремой.

3. Разработана модель угроз целостности среды выполнения процессов, основанная на определение дескрипторов оценки безопасности состояний состоящих из восьми логических переменных В таблице 3 автореферата приведены критерии идентификации угроз по семи угрозам. Реально их намного больше и только в базе данных угроз ФСТЭК их 18, Всего для среды виртуализации их более 80. Каким образом достигается гарантированная защита для всех угроз? Достаточно ли количество переменных дескрипторов для описания появления угроз информационной безопасности ? Эти вопросы требуют ответа.
4. Разработан и достаточно обоснован метод реактивной защиты суперкомпьютеров, при попадании вычисленного дескриптора в зону риска. Это позволяет контролировать контекст и тайминг выполняемых операций в недоверенной аппаратуре.
5. Разработан и исследован метод реконфигурации среды выполнения про активные защиты суперкомпьютера.
6. Разработана методика тестирования уровня защищенности основанная на алгоритме «маркированного» сканирования, позволяющие повысить уровень защищенности вычислительных ресурсов суперкомпьютера и минимизировать ошибки первого и второго рода.

Основные положения диссертации, выносимые на защиту, подтверждаются разработанной автором методикой тестирования и результатами представленными в таблицах 8,9.

Диссертация соответствует критериям, предъявляемыми к докторским диссертациям и установленным Положением «О присуждении учёных степеней ФГАОУ ВО «Южный федеральный университет», а её автор - Моляков А.С. заслуживает присуждения учёной степени доктора технических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Профессор кафедры безопасности и информационных технологий Инженерно-экономического института НИУ «МЭИ», доктор технических наук

Минзов Анатолий Степанович
E-mail: minzovas@mpei.ru

Подпись профессора Минзова Анатолия Степановича заверяю
Заместитель начальника управления по работе с персоналом НИУ «МЭИ»

Полевая Л.И.