ОТЗЫВ

на автореферат диссертации Молякова Андрея Сергеевича «Модели и методы 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», технические науки

Актуальность диссертации Молякова А.С. объясняется тем, что классический подход контроля доступа предполагает использование атрибутов (прав) доступа в запросах к этим объектам на выполнение некоторых операций над ними. Если проверка таких атрибутов оказывается успешной, то доступ к объекту на его уровне защиты разрешается, далее выполняется запрашиваемая операция над ним.

При таком подходе оказывается технически возможным перехват запроса и использование его прав доступа в подменяющем его запросе, нацеленном на вредоносное воздействие. Более того, существующие и успешно внедрённые программно-технические решения промышленного комплекса России ориентированы на традиционные вычислительные кластеры и не учитывают специфики суперкомпьютеров.

Особенности и новизна принципов защиты:

1. Разработка, тестирование и верификация прикладного и системного программного обеспечения осуществляется в многоуровневой «песочнице» с контролем контекста и тайминга выполнения запросов (операций).
2. Проверка на наличие непустых команд.
3. Формируется очередь запросов. Анализируется процесс прохождения запросов с первого уровня по восьмой. Если меняется фрейм запроса в процессе его обработки, то происходят изменения значащих битов тегированных полей.
4. Ограничение на повышение уровня привилегий за счет появления значащего бита.

5. Введены тегированные поля индикация обращения к привилегированным областям памяти.

6. Вычисляется уникальный id для каждого процесса в виде хеш-значения.

7. Анализируются «трассы выполнения команд» с учетом переключений всех возможных режимов работы процессора в виде набора меток (маркеров).

8. Синхронизация реализована с помощью гипервизора с поддержкой расширенных префиксных команд в качестве прослойки между гостевыми и управляющими операционными системами и контроллером транзакционной памяти.

9. На этапе подготовки к запуску задач осуществляется создание снимков запускаемых процессов и сохранение их в таблице гипервизора в виде массива строк-ключей для вычисления результирующей сверки хеш-функции.

10. Цикл мониторинга ссылок безопасности представляет собой 8 интервалов наблюдений и 8 контрольных измерений. Шаг квантования кратен 1/8.

11. Алгоритм вычислений дескрипторов безопасности зависит от времени. Адаптация к потоку входных данных.

Теоретическая значимость состоит в том, что решена важная научная проблема супервентности. Разработаны теоретические и научно-методические принципы защиты суперкомпьютеров с использованием средств виртуализации, основанные на построении и формализации универсальных и равномерных функций оценки безопасных состояний суперкомпьютеров для заданных классов операций, отличающиеся нахождением в n-мерной алгебраической системе инварианта.

Практическая значимость заключается в разработке технологии и программно-технических средств на основе предложенных моделей и методов, составляющих принципы реактивной и проактивной защиты. 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 суперкомпьютеров.

Следует особо отметить важность диссертационной работы для промышленной отрасли России, поскольку предложенные и разработанные автором модели и методы, методика и технология позволяют обеспечивать контроль защищенности информации в крупных высокопроизводительных промышленных кластерах и других супер-ЭВМ, быстро и эффективно проводить аудит защищенности АСУ ТП, в частности:

- обеспечивать выявление, анализ уязвимостей и предлагать меры по оперативному устранению вновь выявленных уязвимостей;
- обеспечивать контроль установки обновлений программного обеспечения для компонентов АСУ;
- обеспечивать контроль параметров настройки ПО АСУ;
- обеспечивать контроль состава технических средств и ПО АСУ.

В автореферате содержатся основные результаты и выводы, полученные соискателем в ходе самостоятельных исследований.

Проведенное исследование и полученные в его ходе результаты соответствуют п. 3 и п. 15 определения специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» паспорта специальностей ВАК (технические науки).

По структуре и содержанию автореферата нет серьезных недостатков. Оформление соответствует установленным требованиям и включает в себя все необходимые разделы.

В качестве замечаний отмечу:

1) При обзоре законодательства в части обеспечения информационной безопасности объектов КИИ в автореферате приведен только 187-ФЗ.

2) Не представлено сравнение авторских методов с нейросетевыми методами и методами поведенческого анализа идентификации угроз.

Диссертационная работа Молякова Андрея Сергеевича «Модели и методы обеспечения информационной безопасности стационарных и бортовых вычислительных систем» соответствует критериям, предъявляемым к докторским диссертациям и 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».

Доктор физико-математических наук, профессор, профессор кафедры информационных технологий, искусственного интеллекта и общественно-социальных технологий цифрового общества

Андрей Евгеньевич Краснов

Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский государственный социальный университет»
129226, г. Москва, ул. Вильгельма Пика д. 4 стр. 1.
info@rgsu.net, +7 (495) 255-67-67

ПОДПИСЬ Краснова А.Е.
УДОСТОВЕРЯЮ
СПЕЦИАЛИСТ
ПО КАДРАМ
ДИМОВА