Экз.№ 1

МИНИСТЕРСТВО ОБОРОНЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБОРОНЫ РОССИИ)
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
КАЗЁННОЕ ВОЕННОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
ВОЕННАЯ АКАДЕМИЯ
РАКЕТНЫХ ВОЙСК СТРАТЕГИЧЕСКОГО
НАЗНАЧЕНИЯ
имени Петра Великого

г. Балашиха, 143900

« 1 » 03 2024 г. № 10/37/1

УТВЕРЖДАЮ
заместитель начальника академии
по учебной и научной работе
генерал-майор Р. Ногин
« 1 » февраля 2024 г.

ОТЗЫВ

на автореферат диссертации МОЛЯКОВА Андрея Сергеевича на тему: «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»

Актуальность темы диссертационной работы Молякова А.С. обусловлена объективно существующим противоречием между существующими традиционными направлениями обеспечения информационной безопасности суперкомпьютеров, связанными с увеличенной численностью обслуживающего персонала и использованию методов, суть которых заключается в сигнатурном поиске уже известного вредоносного программного обеспечения с одной стороны и очевидными рисками увеличения уровня внутренних угроз, а также отсутствием гибкости в в использовании и функционировании оборудования и программного обеспечения при совместном функционировании разных операционных систем и ЭВМ с разной архитектурой сборки с другой стороны. В этих условиях исследования вопросов, связанных с обоснованием применения многомодульных мультидоменных гипервизоров, выступающих в роли интегрированной защиты суперкомпьютеров можно отнести к актуальным.

Автором сформулирована следующая **научная проблема**: разработка и внедрение механизмов многоуровневого контроля, представляющих собой модели и методы обеспечения информационной безопасности на основе применения многомодульных мультидоменных гипервизоров, позволяющих создать доверенную среду выполнения программ суперкомпьютеров на

недоверенном оборудовании с возможностью обеспечения надежной защиты от угроз, реализуемых с использованием средств скрытого информационного воздействия.

Результатами, выносимыми на защиту, являются:

теоретические и научно-методические принципы защиты стационарных и бортовых суперкомпьютеров с использованием средств виртуализации;

модель безопасных операций, основанная на декомпозиции информационных процессов в виде 8-ми уровневой иерархической структуры и принципах кибериммунитета;

модель угроз целостности среды выполнения процессов, основанная на новой парадигме написания правил политики безопасности;

метод реактивной защиты суперкомпьютеров, основанный на виртуализации среды выполнения процессов, если вычисленный дескриптор состояния попадает в зону «риска»;

метод реконфигурации среды выполнения проактивной защиты суперкомпьютеров, основанный на парадигме темпоральной логике для проверки истинности принимаемых решений на структурах Крипке;

программно-технические решения, основанные на разработанных моделях и методах.

Научная новизна результатов работы, исходя из содержания автореферата, заключается:

в разработке новой парадигмы написания правил политики безопасности, отличающейся возможностью задания сущностей вместо классической связки «субъект, объект, предикат» – «субъект», «объект» и «дескриптор оценки безопасности состояний»;

в предложенном подходе декомпозиции информационных процессов в виде 8-ми уровневой иерархической структуры с обоснованием оценки безопасности состояния в виде логической функции и проверки истинности принимаемых решений на каждой возможной интерпретации с учетом спецификации суперкомпьютеров в виде временной и пространственной сложности;

в предложенном методе реактивной защиты суперкомпьютеров, в основу которого положено применение траекторий вычислений дескрипторов оценки безопасности состояний на структурах Крипке;

в предложенном методе реконфигурации среды выполнения проактивной защиты суперкомпьютеров, основанном на парадигме темпоральной логике для проверки истинности принимаемых решений на структурах Крипке, с появившейся возможностью вычисления доверительной вероятности в качестве показателя защищенности компонентов среды на наборах тегерированных данных;

в представленной методике тестирования уровня защищенности, основанной на алгоритме «маркерного» сканирования, в которой предложено

использование набора меток путем сопоставления признаков скрытых угроз и действий сочетаниям меток.

Обоснованность и достоверность научных положений, выводов и предложений обеспечивается корректностью применения известных методов исследований, совпадением результатов теоретических исследований и практических действий, их внутренней непротиворечивостью и адекватностью физическим представлениям об исследуемом процессе, а также соответствующими актами внедрения (реализации), схемами и чертежами рабочей конструкторской документации.

Теоретическая значимость работы заключается в дальнейшем развитии теории информационной безопасности, в части, касающейся формализации информационных процессов суперкомпьютеров в виде «вычисляемой свертки состояний среды выполнения», предложены новые теоретические и научно-методические принципы для создания защищенных суперкомпьютеров. Сформулировано и обосновано условие разрешимости проблемы установки логического соответствия между изменениями программ среды исполнения суперкомпьютера и изменениями компонентов аппаратуры.

Практическая ценность работы состоит в том, что предложенная технология следящих действий со стороны гипервизоров и управляющих операционных систем суперкомпьютеров, основанная на использовании проксирующих модулей и верификатора команд позволяет повысить уровень защищенности суперкомпьютеров, а разработанные в рамках проведённых исследований программно-технические решения, основанные на разработанных моделях и методах, отличающиеся 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),позволяющие реализовать гарантированно защищенные системы, адаптированные к потоку входных данных и набором конфигураций вычислительной среды.

Результаты работы исходя из автореферата достаточно полно **апробированы** на 12 научно-технических и научно-практических конференциях и семинарах, в том числе и с международным участием.

Положения, выносимые на защиту **опубликованы** автором в 31 научной работе, в том числе в 10 статьях в рецензируемых научных изданиях, рекомендованных ВАК России к опубликованию, в 6 статьях, представленных в изданиях, индексируемых Scopus, в свидетельстве о государственной регистрации программ для ЭВМ, а также в 2 патентах на изобретение.

Отмечая несомненные достоинства диссертационного исследования, необходимо указать, что, судя по автореферату, работа не лишена недостатков. Основными из них являются:

отсутствие формализованной постановки научной проблемы в явном виде существенно затрудняет объективную оценку степени достижения поставленной цели и решения научной проблемы;

автор в автореферате неоднократно делает заключение о создании гарантированно защищенных систем, при этом в качестве показателя, характеризующего степень гарантированной защищенности выбрана некоторая вероятность, порядок определения которой в автореферате не определен;

при описании доказательства теоремы о равномерной перечислимой функций суперкомпьютера автор не описывает, что он понимает под функциями суперкомпьютера, кроме того, в ходе практических вычислений автор оперирует аргументами, имеющими различное смысловое и символьное значение. Так, например, на стр. 12 в третьем абзаце приводится описание N – числа вложенности пространства вычислений, а уже в седьмом абзаце N выступает в качестве числа уровней иерархии, а уже на стр. 25 настоящего автореферата, в последнем абзаце N выступает в качестве числа уровня защиты. Далее автор, в рамках доказательства теоремы приводит ряд значений некоторой величины Q с отсылкой к выражению (4), которое такового не содержит, но имеет отсылку к величине, обратной доверительной вероятности – q, которую, по всей видимости, автор и имел ввиду;

представленные в автореферате методы реактивной и проактивной защиты носят в целом декларативный характер, а объем автореферата не дает возможности провести оценку результатов сравнительного анализа эффективности предложенных и существующих методов проактивной защиты, таких как, например, метод поведенческого анализа, метод ограничения выполнения операций, методы контроля целостности программного обеспечения и операционной системы, методы предотвращения вторжений (HIPS и VIPS) и т.д., автор ограничился констатацией того, что ни один из рассмотренных им методов не адаптирован для решения задач идентификации и блокирования угроз информационной безопасности с учетом спецификации суперкомпьютеров;

автором получены два патента на изобретение, но установить их роль в решении вскрытой научной проблемы затруднительно, так как исходя из автореферата их содержание раскрыто только в Приложениях к диссертации, там же находится набор программно-инструментальных средств экспериментального стенда, что по мнению авторов настоящего отзыва вызывает сожаление, так как именно структура экспериментального стенда, методика эксперимента и его результаты существенно повысили бы адекватность моделирования, значимость и законченность проводимых исследований.

Данные недостатки не влияют на общий положительный вывод по диссертации.

Выводы:

в целом, диссертационная работа Молякова А.С. характеризуется высоким научным уровнем, содержит ряд оригинальных подходов к исследованию и научных результатов, ценных как в теоретическом, так и в практическом отношении. Автореферат написан лаконичным языком, в целом, дает возможность сформировать представление о работе. Тема и содержание автореферата соответствует паспорту специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»;

судя по автореферату, диссертация является выполненной автором самостоятельно научно-квалификационной работой, содержащей новые научные результаты, выдвигаемые для публичной защиты, отвечает критериям, установленным п. 9 «Положения о присуждении ученых степеней» (постановления Правительства РФ от 24.09.2013 г. № 842, , предъявляемым к диссертациям на соискание ученой степени доктора наук, 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».

Начальник кафедры №37
доктор технических наук

«1» марта 2024 г. Щербаков Виталий Алексеевич

Доцент кафедры №37
кандидат технических наук

«1» марта 2024 г. Новиков Артем Николаевич