ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА ЮФУ801.02.02

созданного на базе федерального государственного автономного образовательного учреждения высшего образования «Южный федеральный университет» Минобрнауки России, по диссертации на соискание ученой степени доктора наук

аттестационное дело № _____,
решение диссертационного совета
от 28 марта 2024 г. № 28

О присуждении Молякову Андрею Сергеевичу, гражданину Российской Федерации, ученой степени доктора технических наук.

Диссертация «Модели и методы обеспечения информационной безопасности стационарных и бортовых суперкомпьютерных вычислительных систем» по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность» принята к защите 16 ноября 2023 г. (протокол заседания № 20) диссертационным советом ЮФУ801.02.02, созданным на базе федерального государственного автономного образовательного учреждения высшего образования «Южный федеральный университет» в соответствии с приказами № 173-ОД от 30.06.2022 г., № 121-ОД от 28.04.2023 г.

Соискатель Моляков Андрей Сергеевич, 16.11.1982 года рождения, в 2006 г. окончил федеральное государственное бюджетное образовательное учреждение высшего образования «Российский государственный гуманитарный университет» по специальности «Комплексная защита объектов информатизации». В 2014 г. окончил аспирантуру федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный политехнический университет» по направлению подготовки 10.06.01 «Информационная безопасность» (направленность: Методы и системы защиты информации, информационная безопасность).

Диссертацию на соискание ученой степени кандидата технических наук на тему «Средства противодействия скрытым угрозам информационной безопасности в среде облачных вычислений» по специальности 05.13.19 «Методы

и системы защиты информации, информационная безопасность» защитил в 2014 г. в диссертационном совете Д212.229.27, созданном на базе федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный политехнический университет».

С 2018 г. по настоящее время работает в должности доцента кафедры комплексной защиты информации факультета информационных систем и безопасности Института информационных наук и технологий безопасности в федеральном государственном бюджетном образовательном учреждении высшего образования «Российский государственный гуманитарный университет».

Диссертация выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Российский государственный гуманитарный университет» на кафедре комплексной защиты информации.

Соискатель представил диссертацию к защите без научного консультанта.

Официальные оппоненты:

1. **Конявский Валерий Аркадьевич,** доктор технических наук, федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (национальный исследовательский университет)», г. Долгопрудный, заведующий кафедрой «Защиты информации»;

2. **Лепешкин Олег Михайлович,** доктор технических наук, доцент, федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи имени маршала Советского Союза С.М. Буденного», г. Санкт-Петербург, доцент кафедры безопасности инфокоммуникационных систем специального назначения;

3. **Петренко Сергей Анатольевич,** доктор технических наук, профессор, Автономная некоммерческая организация высшего образования «Университет Иннополис», г. Иннополис, профессор Центра информационной безопасности,

дали **положительные отзывы** на диссертацию.

Соискатель имеет 56 опубликованных работ, в том числе по теме диссертации опубликовано 31 научных печатных работ, из которых 10 – в ведущих рецензируемых научных изданиях, входящих в перечень ВАК РФ; 6 – в международных изданиях, индексируемых Scopus; 15 – в материалах конференций и других научных изданиях. Также автором получено 2 патента РФ на изобретения и 1 свидетельство о государственной регистрации программы для ЭВМ.

Наиболее значимые научные работы по теме диссертации:

1. Моляков, А. С. Исследование скрытых механизмов управления задачами ядра Windows NT 5.1 / А. С. Моляков // Известия ЮФУ. Технические науки. – 2007. – № 4(76). – С. 139-147 (входит в перечень ВАК).

В работе Моляковым А. С. проведено исследование скрытых механизмов управления задачами ядра Windows NT 5.1, показаны недостатки мандатной и дискреционной политик безопасности, даны рекомендации по повышению уровня защищенности автоматизированных рабочих мест на базе платформы Windows и предложена методика тестирования.

2. Моляков, А. С. Новый метод систематического поиска недекларированных возможностей ядра Windows NT 5.1 с введением контроля ContextHooking и PspCidHooking / А. С. Моляков // Вопросы защиты информации. – 2008. – № 1(80). – С. 49-56 (входит в перечень ВАК).

В работе Моляковым А. С. проведен обзор программных инструментов динамического и статического анализа на примере Stack Guard, Valgrind Memcheck, Intel Memory Checker, Flow Finder, RATS, Pscan, UNO, Flexe Lint, предложен и описан новый метод систематического поиска недекларированных возможностей ядра Windows NT 5.1, основанный на контроле контекста выполнения процессов на уровне планировщика задач ядра и диспетчера работы с оборудованием.

3. Моляков, А. С. Метод контроля отображения защищенных сегментов памяти при трансляции виртуальных адресов процессов ОС Windows / А. С.

Моляков // Вопросы защиты информации. – 2008. – № 2(81). – С. 32-35 (входит в перечень ВАК).

В работе Моляковым А. С. разработан метод контроля сегментов памяти при трансляции адресов, основанный на использовании технологии аппаратной виртуализации. Взаимодействие процессов пользователя происходит с компонентами гипервизора, который создает изолированную среду выполнения команд.

4. Моляков, А. С. KPROCESSOR_CID_TABLE -факторинг – новое направление в теории компьютерного анализа вирусного кода и программных закладок / А. С. Моляков // Проблемы информационной безопасности. Компьютерные системы. – 2009. – № 1. – С. 7-18 (входит в перечень ВАК).

В работе Моляковым А. С. предложено новое концептуальное направление в теории компьютерного анализа вирусного кода и программных закладок, основанное на контроле доступа по набору характерных признаков – маркеров, представленных в виде кортежей логических переменных, приведены результаты экспериментальных исследований по оценке эффективности.

5. Моляков, А. С. KPROCESSOR-CID-table-факторинг в области создания защищенных ОС нового поколения / А. С. Моляков // Безопасность информационных технологий. – 2009. – Т. 16, № 4. – С. 125-129 (входит в перечень ВАК).

В работе Моляковым А. С. предложен новый подход в области создания защищенных операционных систем нового поколения. Работа с тегами запросов на разных уровнях защиты производится модулями гипервизора. Атрибуты доступа к объекту и привилегии субъекта, связи между ними формализованы в виде конъюнкции предикатов.

6. Моляков, А. С. Модель скрытых угроз информационной безопасности в среде облачных вычислений / А. С. Моляков, В. С. Заборовский, А. А. Лукашин // Проблемы информационной безопасности. Компьютерные системы. – 2014. – № 2. – С. 41-46 (входит в перечень ВАК, 83 % авторских).

В работе Моляковым А. С. проведен анализ угроз безопасности в среде облачных вычислений, разработана модель скрытых угроз и предложена новая парадигма написания правил политики безопасности.

7. Моляков, А. С. Мультиграфовая модель операций для защиты среды облачных вычислений от скрытых угроз информационной безопасности / А. С. Моляков, В. С. Заборовский, А. А. Лукашин // Проблемы информационной безопасности. Компьютерные системы. – 2014. – № 2. – С. 37-40 (входит в перечень ВАК, 75 % авторских).

В работе Моляковым А. С. разработана мультиграфовая модель операций, позволяющая повысить уровень защищенности среды облачных вычислений от скрытых угроз информационной безопасности, формализована и описана функция оценки безопасности состояний, заданная на наборе кортежей логических переменных.

8. Моляков, А. С. Разработка прототипа вычислительного устройства с не фон-Неймановской архитектурой на базе отечественного микропроцессора стратегического назначения J7 / А. С. Моляков // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 1. – С. 22-28 (входит в перечень ВАК).

В работе Моляковым А. С. разработана подсистема обеспечения информационной безопасности суперкомпьютера «Ангара», представлены структурные и функциональные схемы прототипа вычислительного устройства на базе отечественного перспективного процессора J7 с не фон-Неймановской архитектурой.

9. 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 (входит в перечень ВАК).

В работе Моляковым А. С. разработан метод реактивной защиты суперкомпьютеров, предложена технология выявления уязвимостей, которая

позволяет создать доверенную среду вычислений с полным контролем контекста и тайминга выполняемых операций на недоверенной аппаратуре.

10. 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 (входит в перечень ВАК).

В статье Моляковым А. С. проведено аналитическое исследование литературных источников и современных методов защиты суперкомпьютеров, предложен инновационный вариант развития защищенных супер-ЭВМ с использованием реконфигурируемых гибридных вычислителей (ускорителей) для решения важных задач фундаментальной медицины и инженерии в России, представлены результаты экспериментальных исследований.

11. Molyakov, A. S. Model of hidden IT security threats in the cloud computing environment / A. S. Molyakov, V. S. Zaborovsky, A. A. Lukashin // Automatic Control and Computer Sciences. – 2015. – Vol. 49, No. 8. – P. 741-744. – DOI 10.3103/S0146411615080295 (входит в базу Scopus, 75 % авторских).

В работе Моляковым А. С. проведен анализ актуальных угроз информационной безопасности для распределенных облачных сред, разработана модель угроз целостности среды выполнения процессов, основанная на новой парадигме написания правил политики безопасности, предложено формализованное описание угроз в виде конъюнкции предикатов из восьми логических переменных, заданы параметры функции оценки безопасности состояний.

12. Molyakov, A. S. Token scanning as a new scientific approach in the creation of protected systems: A new generation OS MICROTEK / A. S. Molyakov // Automatic Control and Computer Sciences. – 2016. – Vol. 50, No. 8. – P. 687-692. – DOI 10.3103/S0146411616080149 (входит в базу Scopus).

В работе Моляковым А. С. разработана модель безопасных операций, основанная на декомпозиции информационных процессов в виде 8-уровневой

иерархической структуры и принципах кибериммунитета, описаны критерии верификации принимаемых решений на каждой возможной интерпретации с учетом специфики суперкомпьютеров.

13. 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 (входит в базу Scopus).

В работе Моляковым А. С. разработан прототип суперкомпьютера «нового поколения». Вычислительные узлы строятся на специальных многоядерных мультитредово-потоковых микропроцессорах и вычислительных блоках любой другой архитектуры, объединяются в модули в виде многосокетных плат и могут работать над логически единой адресуемой памятью (глобально адресуемой памятью), образуемой локальными памятями модулей с вычислительными узлами. Управление сервисными и вычислительными узлами, объединенными высокоскоростными линками сети (например, российская отказоустойчивая сеть «Ангара»), осуществляется с помощью защищенного распределенного мультидоменного гипервизора.

14. 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 (входит в базу Scopus).

В работе Моляковым А. С. разработана методика тестирования уровня защищенности, основанная на алгоритме «маркерного» сканирования с использованием набора меток, приведены результаты экспериментальных исследований по оценке уровня защищенности и производительности.

15. 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 (входит в базу Scopus).

В работе Моляковым А. С. разработан метод реконфигурации среды выполнения проактивной защиты суперкомпьютеров, основанный на парадигме темпоральной логики для проверки истинности принимаемых решений на структурах Крипке, заданы критерии идентификации, позволяющие на ранней стадии обнаруживать новые классы уязвимостей и противодействовать им путем автоматической реконфигурации структуры.

16. 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 (входит в базу Scopus).

В работе Моляковым А. С. разработана технология организации доверенной среды вычислений стационарных и бортовых вычислительных систем в условиях роста угроз безопасности для российских суперкомпьютерных платформ «Ангара» серии ЕС1740.

На диссертацию и автореферат поступило 12 отзывов: 11 положительных, 1 отрицательный. Во всех отзывах отмечено, что диссертационная работа соответствует паспорту специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность», технические науки.

1) ФГБОУ ВО «Уфимский университет науки и технологий», г. Уфа, отзыв подписал профессор кафедры «Вычислительная техника и защита информации», доктор технических наук, профессор Машкина И. В., 1 замечание;

2) ФГБУ «Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России» (федеральный центр науки и высоких технологий), г. Москва, отзыв подписал главный научный сотрудник, доктор физико-математических наук, профессор Прус Ю. В., 1 замечание;

3) ФГКВОУ ВО «Военная академия воздушно-космической обороны имени Маршала Советского Союза Г. К. Жукова», г. Тверь, отзыв подписал профессор 6 кафедры, доктор технических наук, доцент Дроботун Е. Б., 2 замечания;

4) ФГБОУ ВО «Южно-Российский государственный политехнический университет имени М. И. Платова», г. Новочеркасск, отзыв подписал заведующий кафедрой «Информационная безопасность», кандидат военных наук, доцент Баранов В. В., 1 замечание;

5) ФГКОУ ВО «Московский университет Министерства внутренних дел Российской Федерации имени В. Я. Кикотя», г. Москва, отзыв подписал профессор кафедры информационной безопасности, кандидат технических наук Плотников Г. Г., 1 замечание;

6) ФКУ НПО «Специальная техника и связь» Министерства внутренних дел Российской Федерации, г. Москва, отзыв подписал ведущий научный сотрудник направления по взаимодействию с Военно-промышленной комиссией РФ, кандидат технических наук Антышев А. А., 2 замечания;

7) ФГКВОУ ВО «Военная академия ракетных войск стратегического назначения имени Петра Великого», г. Балашиха, отзыв подписали начальник кафедры № 37, доктор технических наук Щербаков В. А., доцент кафедры № 37, кандидат технических наук Новиков А. Н., 5 замечаний;

8) ФГБУ «4 Центральный научно-исследовательский институт Министерства обороны Российской Федерации», г. Королев, отзыв подписали старший научный сотрудник, кандидат технических наук Купин С. В., главный научный сотрудник, доктор технических наук, профессор Климов С. М., начальник научно-исследовательского отдела, кандидат технических наук Антонов С. Г., 4 замечания.

9) ФГБОУ ВО НИУ «Московский энергетический институт», отзыв подписал профессор кафедры безопасности и информационных систем Инженерно-экономического института, доктор технических наук Минзов А. С., 2 замечания;

10) ФГБОУ ВО «Россиийский государственный социальный университет», отзыв подписал профессор кафедры информационных технологий, искусственного интеллекта и общественно-социальных технологий цифрового

общества, доктор физико-математических наук, профессор Краснов А. Е., 2 замечания;

11) ФГАОУ ВО «Уральский федеральный университет им. первого Президента России Б. Н. Ельцина», отзыв подписал директор Учебно-научного центра «Информационная безопасность», доктор технических наук, профессор Поршнев С. В., 7 замечаний;

12) ФГБОУ ВО «Оренбургский государственный университет», отзыв подписала доцент кафедры «Вычислительная техника и защита информации», кандидат педагогических наук, доцент Бурькова Е. В., 1 замечание.

Наиболее существенные замечания:

1. Концептуальную постановку научных задач и проблемы во введении необходимо было дополнить формальным представлением по схеме «дано – необходимо найти – ограничения».

2. В тексте диссертации автор подробно описал разные профили защиты, наборы конфигураций среды исполнения программ и домены защиты для трех типов стационарных суперкомпьютеров, но меньше внимания уделил описанию программно-технических решений для бортовых супер-ЭВМ.

3. При описании методики тестирования и алгоритма «маркерного» сканирования автором достаточно хорошо и информативно проиллюстрированы разработанные принципы и подходы, однако местами изложение немного фрагментарное, не освещены подробно решения при работе с бортовыми супер-ЭВМ и крупными промышленными кластерами, например, с широко используемыми высокопроизводительными вычислительными модулями серии «Багет Р2А».

Выбор официальных оппонентов обосновывается их достижениями в данной отрасли науки и способностью определить научную и практическую ценность диссертации. Доктор технических наук Конявский Валерий Аркадьевич, заведующий кафедрой «Защиты информации» ФГАОУ ВО «Московский физико-технический институт (национальный исследовательский университет)», имеет ученую степень д.т.н. по специальности 05.13.19 «Методы и системы защиты

информации, информационная безопасность», является ведущим специалистом в области информационной безопасности, имеет необходимое количество публикаций в рецензируемых ведущих научных журналах по тематике диссертации. Доктор технических наук, профессор Петренко Сергей Анатольевич, профессор Центра информационной безопасности АНО ВО «Университет Иннополис», имеет ученую степень д.т.н. по специальности 20.02.27 «Информационное противоборство в военной сфере», является специалистом и обладает высокой квалификацией в области информационной безопасности, имеет необходимое количество публикаций в рецензируемых ведущих научных журналах по тематике диссертации. Доктор технических наук, доцент Лепешкин Олег Михайлович, доцент кафедры безопасности инфокоммуникационных систем специального назначения ФГКВОУ ВО «Военная академия связи имени Маршала Советского Союза С.М. Буденного», имеет ученую степень д.т.н. по специальности 05.13.10 «Управление в социальных и экономических системах», является специалистом и обладает высокой квалификацией в области информационной безопасности, имеет необходимое количество публикаций в рецензируемых ведущих научных журналах по тематике диссертации.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований получены следующие научные результаты, обладающие новизной и свидетельствующие о личном вкладе соискателя:

– системно-архитектурный подход в области создания доверенной среды вычислений суперкомпьютеров, **основанный** на методологии управления процессами аппаратными гипервизорами и контроллерами транзакционной памяти, **отличающийся** построением и формализацией алгоритмических решений мониторинга обработки запросов на всех уровнях иерархии, **позволяющий** решить научную проблему супервентности (безопасности взаимосвязанных интерфейсных слоев);

– модель угроз целостности среды выполнения процессов, **основанная** на новой парадигме определения правил политик безопасности, **отличающаяся** заданием сущностей «субъект», «объект» и «дескриптор оценки безопасности

состояний» вместо классической связки «субъект, объект, предикат», **позволяющая** описать и формализовать каждую i-ую угрозу аргументов в виде конъюнкции предикатов из восьми логических переменных, что упрощает процесс идентификации угроз;

– модель безопасных операций, **основанная** на декомпозиции информационных процессов в виде 8-уровневой иерархической структуры и принципах кибериммунитета, **отличающаяся** оценкой безопасности состояний в виде логической функции контроля доступа и проверкой истинности принимаемых решений на каждой возможной интерпретации правил политик безопасности с помощью математических выражений темпоральной логики, **позволяющая** идентифицировать и блокировать разные классы уязвимостей на всех уровнях иерархии выполнения запросов;

– метод реактивной защиты суперкомпьютеров, **основанный** на виртуализации среды выполнения процессов, если вычисленный дескриптор состояния попадает в зону «риска», **отличающийся** применением траекторий вычислений дескрипторов оценки безопасности состояний на структурах Крипке, **позволяющий** создать единую технологию выявления уязвимостей и реализовать полный контроль контекста и тайминга выполняемых операций на недоверенной аппаратуре;

– метод реконфигурации среды выполнения проактивной защиты суперкомпьютеров, **основанный** на парадигме темпоральной логики для проверки истинности принимаемых решений на структурах Крипке, **отличающийся** вычислением доверительной вероятности в качестве показателя защищенности компонентов среды на наборах тегированных данных в виде согласованной вариации факторных и результативных признаков, **позволяющий** на ранней стадии обнаруживать новые классы уязвимостей и противодействовать им путем автоматической реконфигурации структуры;

– методика тестирования уровня защищенности, **основанная** на алгоритме «маркерного» сканирования, **отличающаяся** использованием набора меток: сочетаниям меток сопоставляются признаки скрытых угроз и действия,

отвечающие требованиям выбранной политики информационной безопасности, **позволяющая** повысить уровень защищенности вычислительных ресурсов суперкомпьютеров и минимизировать ошибки 1-го и 2-го рода;

– оригинальность и новизна рационализаторских и изобретательских предложений в части построения архитектуры защищенных вычислительных модулей супер-ЭВМ подтверждены получением двух патентов на изобретения.

Теоретическая значимость исследования обоснована тем, что:

– в работе введено новое понятие «дескриптор оценки безопасности состояний системы», базирующееся на формализации информационных процессов суперкомпьютеров в виде «вычисляемой свертки состояний среды выполнения». В качестве спецификации системы используется структура Крипке;

– предложены модели и методы реактивной и проактивной защиты, которые развивают дисциплину информационной безопасности. Судя по открытым международным и отечественным источникам, исследования стационарных и бортовых суперкомпьютеров в качестве объектов защиты проводятся впервые;

– сформулированы и подтверждены гипотезы, связывающие критичность атакуемых компонентов суперкомпьютеров и характеристики моделирующих графов. Правила политики безопасности заданы в виде модальных структур темпоральной логики CTL, учитывающих контекст выполнения и тайминг операций (запросов);

– выявлены закономерности в характере зависимости между уровнем устойчивости к атакам, направленным на удаление путей реализации целевой функции, и избыточностью системы на уровне межкомпонентных связей;

– доказано, что предложенные методы повышают уровень гарантированной защищенности стационарных и бортовых суперкомпьютеров.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что разработанные автором модели, методы, методика и технология нашли применение при решении прикладных задач в области создания отечественной элементной базы и системного программного

обеспечения для суперкомпьютеров высшего диапазона производительности, что, согласно «Стратегии научно-технологического развития Российской Федерации», является важнейшим направлением развития отрасли промышленности. Разработаны и запатентованы программно-технические решения в виде многомодульного защищенного мультидоменного гипервизора, основанные на разработанных моделях и методах, которые, в отличие от существующих сертифицированных гипервизорных решений, позволяют получить наилучшие показатели производительности, защищенности и не допускают аварийных завершений критических процессов из-за компьютерных атак. Эффективность обнаружения атак на основе авторской методики на 86 процентов выше по сравнению с классическими подходами, при этом ошибки 1-го и 2-го рода не превышают пороговое значение 0,014, а потери производительности составляют менее 6-7 процентов.

Результаты диссертации использованы:

– при разработке вычислительного модуля программно-технического комплекса «Альфа-монитор» для российских суперкомпьютерных платформ «Ангара» серии ЕС1740 и создании подсистемы обеспечения информационной безопасности на базе монитора безопасности и гипервизорных модулей (проксирующих модулей и верификатора команд). Применение результатов отражено в справке о внедрении результатов диссертационной работы, утвержденной проректором по научной работе ФГБОУ ВО «Российский государственный гуманитарный университет» Павленко О. В. от 18.10.2018;

– при разработке ТТЗ на ОКР по созданию семейства унифицированных мобильных вычислительных средств на основе отечественных микропроцессоров для систем и комплексов вооружения, функционирующих в реальном масштабе времени, морского, наземного и воздушного базирования. Применение результатов отражено в акте реализации научных исследований, утвержденном заместителем начальника ФГБУ «3 ЦНИИ» Минобороны России по научной работе Волковым А. В. от 21.12.2022;

– в деятельности лаборатории компьютерной техники и средств защиты информации ИИНТБ ФГБОУ ВО «Российский государственный гуманитарный университет» в ходе разработки новых методов и методики для обеспечения информационной безопасности суперкомпьютерных вычислительных систем в виде экспериментального стенда. Применение результатов отражено в справке о внедрении научно-технологических результатов диссертации, утвержденной проректором по научной работе ФГБОУ ВО «Российский государственный гуманитарный университет» Павленко О. В. № 1703-22/58 от 18.11.2019;

– в учебном процессе на кафедре комплексной защиты информации ФГБОУ ВО «Российский государственный гуманитарный университет» для подготовки студентов направления бакалавриата 10.03.01 «Информационная безопасность» в рамках дисциплин «Программно-аппаратные средства защиты информации. Основная часть», «Актуальные тенденции в области защиты информации», «Безопасность операционных систем». Применение результатов отражено в справке о внедрении теоретических и методических результатов диссертации, утвержденной проректором по научной работе ФГБОУ ВО «Российский государственный гуманитарный университет» Павленко О. В. № 1703-22/59 от 18.11.2019.

По теме диссертации автором получены **патенты на изобретения:**

– 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.;

– 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.

Обоснованность и достоверность полученных в диссертационной работе научных результатов подтверждена корректностью и непротиворечивостью применения математического аппарата, результатами

многочисленных вычислительных экспериментов, опубликованными работами, а также использованием в различных организациях, что подтверждается соответствующими актами. Результаты диссертации докладывались и обсуждались на международных научно-технических и научно-практических конференциях, на которых Моляков А. С. выступал с докладами по данной проблематике и получил положительные отзывы научной общественности.

Личный вклад соискателя состоит в выполнении всех этапов диссертационного исследования:

- постановка и формулировка научной проблемы, выбор интегрального показателя в виде результирующей свертки, которая вычисляется на основе атрибутов протекающих процессов;
- методическая схема исследований, анализ свойств бортовых и стационарных суперкомпьютерных вычислительных систем и определение специфики защиты супер-ЭВМ;
- разработка модели угроз целостности среды выполнения процессов с формализованным описанием каждой i-ой угрозы аргументов в виде конъюнкции предикатов из восьми логических переменных;
- разработка модели безопасных операций, основанной на декомпозиции информационных процессов в виде 8-уровневой иерархической структуры и принципах кибериммунитета;
- разработка и исследование метода реактивной защиты суперкомпьютеров с применением траекторий вычислений дескрипторов оценки безопасности состояний на структурах Крипке;
- разработка и исследование метода реконфигурации среды выполнения проактивной защиты суперкомпьютеров с заданием критериев верификации истинности принимаемых решений на основе математических выражений темпоральной логики;
- разработка технологии создания доверенной среды вычислений суперкомпьютерных систем;
- проведение вычислительных экспериментов и стендовых испытаний.

В диссертации содержится **решение актуальной научной проблемы** – проблемы супервентности, заключающееся в создании доверенной среды вычислений суперкомпьютерных систем в условиях роста угроз безопасности, имеющей значение для развития отрасли знаний «Информационная безопасность» критической информационной инфраструктуры Российской Федерации на примере стационарных и бортовых вычислительных систем.

Разработанные программно-технические средства, математические модели, методы, методика и алгоритм вносят вклад в развитие концептуальных методов информационной безопасности суперкомпьютеров. Предложенные автором диссертации решения научно обоснованы и оценены по сравнению с другими известными решениями.

В диссертации отсутствуют заимствования без ссылок на авторов или источник заимствования. Приведены ссылки на все использованные в диссертации результаты научных работ, выполненные соискателем лично и в соавторстве.

В диссертации отсутствуют недостоверные сведения об опубликованных соискателем работах, в которых изложены основные научные результаты.

Полученные результаты могут быть использованы при выполнении НИОКР, посвященных решению задач обеспечения информационной безопасности при создании стационарных и бортовых суперкомпьютерных систем. Это позволит серьезно продвинуться в разработке защищенных российских суперкомпьютеров и в исследовании перспективных нетрадиционных подходов для обеспечения отрасли промышленности суперкомпьютерами с высокими показателями реальной производительности, защищенности и отказоустойчивости.

Диссертация Молякова Андрея Сергеевича является завершенной научно-квалификационной работой, обладающей теоретической новизной и практической значимостью, внутренним единством, содержит новые научные результаты и положения, свидетельствующие о личном вкладе автора, и соответствует критериям раздела 2 «Положения о присуждении ученых степеней в федеральном государственном автономном образовательном учреждении высшего образования

«Южный федеральный университет» (в редакции от 22.12.2023 г. приказ № 368-ОД), предъявляемым к диссертациям на соискание ученой степени доктора технических наук.

На заседании 28 марта 2024 г. диссертационный совет принял решение присудить **Молякову Андрею Сергеевичу** ученую степень **доктора** технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

При проведении тайного голосования диссертационный совет в количестве 8 человек, из них 7 докторов наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность», участвовавших в заседании, из 10 человек, входящих в состав совета, дополнительно в состав совета никто не вводился, проголосовали:

«за» – 7, «против» – 1, «недействительных бюллетеней» – нет.

Председатель
диссертационного совета Бабенко Людмила Климентьевна

Ученый секретарь
диссертационного совета Ельчанинова Наталья Борисовна
28 марта 2024 г.