ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.087.01
на базе Федерального государственного бюджетного учреждения науки
Институт системного программирования им. В.П. Иванникова
Российской академии наук
Федерального агентства научных организаций РФ
по диссертации на соискание ученой степени кандидата наук

аттестационное дело № _____

решение диссертационного совета от 21 декабря 2017 года № 2017/28

О присуждении Фурсовой Наталье Игоревне, гражданке РФ, ученой степени кандидата технических наук.

Диссертация «Методы мониторинга объектов операционной системы, выполняющейся в виртуальной машине» по специальности 05.13.11 – «математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей» принята к защите 19 октября 2017 г., протокол № 2017/22 диссертационным советом Д 002.087.01 на базе Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность – Федеральное агентство научных организаций), адрес: 109004, г. Москва, ул. А. Солженицына, дом 25, создан Приказом Минобрнауки России о советах по защите докторских и кандидатских диссертаций от 2 ноября 2012 г. № 714/нк.

Соискатель Фурсова Наталья Игоревна, 1989 года рождения, работает инженером в отделе компиляторных технологий Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук, ФАНО.

В 2013 году соискатель окончила Федеральное государственное бюджетное образовательное учреждение высшего образования Новгородский

Государственный университет имени Ярослава Мудрого (НовГУ). В 2016 году соискатель окончила очную аспирантуру НовГУ.

Диссертация выполнена в Новгородском Государственном университете имени Ярослава Мудрого (Министерство образования и науки Российской Федерации) на кафедре информационных технологий и систем.

Научный руководитель – кандидат технических наук Макаров Владимир Алексеевич, Федеральное государственное бюджетное образовательное учреждение высшего образования Новгородский государственный университет имени Ярослава Мудрого, кафедра информационных технологий и систем, начальник управления инноваций.

Официальные оппоненты:

1. Ильин Вячеслав Анатольевич, доктор физико-математических наук, Национальный исследовательский центр "Курчатовский институт", начальник отдела Курчатовского комплекса НБИКС-технологий,
2. Козачок Александр Васильевич, кандидат технических наук, ФГКВОУ ВО "Академия Федеральной службы охраны Российской Федерации", сотрудник ФГКВОУ ВО "Академия Федеральной службы охраны Российской Федерации"

дали положительные отзывы на диссертацию.

Ведущая организация Межведомственный суперкомпьютерный центр Российской академии наук - филиал Федерального государственного учреждения "Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук" (г. Москва) в своем положительном заключении, подписанном Шабановым Борисом Михайловичем (кандидат технических наук, доцент, заместитель директора по научной работе ФГУ ФНЦ НИИСИ РАН, директор МСЦ РАН — филиала ФГУ ФНЦ НИИСИ РАН), указала, что диссертационная работа представляет собой законченную научно-исследовательскую работу, а ее результаты являются полезным вкладом в разработку методов мониторинга объектов операционных систем. Диссертация удовлетворяет всем требованиям ВАК РФ, предъявляемым к

кандидатским диссертациям, а ее автор, Фурсова Наталья Игоревна, заслуживает присуждения ей ученой степени кандидата технических наук по специальности 05.13.11 - математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Выбор официальных оппонентов и ведущей организации обосновывается их компетентностью и достижениями в данной отрасли науки, наличием публикаций в сфере исследований, соответствующей теме диссертации, и способностью определить научную и практическую ценность диссертации.

Соискатель имеет 11 опубликованных работ, в том числе по теме диссертации 7 работ, из них 6 работ опубликованы в рецензируемых научных изданиях.

Публикации посвящены методам мониторинга объектов операционной системы, основанным на использовании двоичного интерфейса приложений. Предложенные методы позволяют выделять высокоуровневую информацию об объектах операционной системы без глубоких знаний об этой системе, а также анализировать встроенные системы. В работах описано и практическое применение предложенных методов.

Наиболее значимые публикации по теме диссертации:

1. Фурсова Н. И., Довгалюк П. М., Васильев И. А., Макаров В. А. Легковесный метод интроспекции виртуальных машин // Programming and Computer Software. — 2017. — № 5. — С. 307—313.

2. Фурсова Н. И., Довгалюк П. М., Васильев И. А. Использование ABI для интроспекции виртуальных машин // Труды Института системного программирования РАН. — 2015. — № 27. — С. 159—168.

3. Fursova N. Introspection of the Virtual Machines with System Calls Monitoring: Student Research Abstract // Proceedings of the 31st Annual ACM Symposium on Applied Computing. — Pisa, Italy : ACM, 2016. —С. 1582—1583. — (SAC ’16). — ISBN 978-1-4503-3739-7. — DOI: 10.1145/2851613.2852008. — URL: http://doi.acm.org/10.1145/2851613.2852008.

Диссертационный совет отмечает, что соискателем получены новые научные результаты:

- разработан метод мониторинга событий виртуальной машины для получения информации об объектах гостевой операционной системы без внедрения инструментального кода на уровне исследуемой системы;
- разработан метод вызова системных функций по запросу анализатора для получения атрибутов объектов операционной системы.

Теоретическая значимость исследования состоит в том, что проведен анализ существующих методов и инструментов мониторинга объектов операционных систем, ыявивший класс нерешенных задач анализа операционных систем телекоммуникационного оборудования (встроенных систем); разработан метод мониторинга объектов операционных систем, позволяющий получать высокоуровневую информацию (о файлах, процессах, модулях и функциях) об объектах операционных систем, выполняющихся в виртуальных машинах. Метод является безагентным, не требует знаний о внутренних структурах и параметрах сборки операционных систем, что позволят производить анализ встроенных систем.

Значение полученных соискателем результатов исследования для практики состоит в том, что разработан набор плагинов для эмулятора QEMU — инструмент для мониторинга объектов операционных систем; разработанный инструмент внедрен в ИСП РАН и используется для получения об объектах операционной системы высокоуровневой информации, необходимой для реализации отслеживания чувствительных данных в исследуемых операционных системах с целью обеспечения их безопасности и для анализа встроенных систем.

Достоверность результатов исследования заключается в том, что полученная с помощью разработанных методов высокоуровневая информация в исследуемой операционной системе была использована в ИСП РАН для отслеживания чувствительных данных в операционной системе и анализа встроенного оборудования телекоммуникационных систем.

Личный вклад соискателя состоит в его определяющем участии в разработке методов мониторинга объектов операционной системы — метода мониторинга событий виртуальной машины и метода вызова системных функций по запросу анализатора. Соискатель принимал непосредственное участие в реализации методов, апробации полученных результатов исследования и подготовке основных публикаций по теме диссертации (в соавторстве с сотрудниками Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук).

На заседании 21 декабря 2017 диссертационный совет принял решение присудить Фурсовой Н.И. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 15 человек, из них 6 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 20 человек, входящих в состав совета, проголосовали: за – 15, против – 0, недействительных бюллетеней – 0.

Заместитель председателя диссертационного совета,
доктор физико-математических наук Томилин А. Н.

Ученый секретарь диссертационного совета,
кандидат физико-математических наук Зеленов С. В.

21 декабря 2017 г.