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

аттестационное дело № _____

решение диссертационного совета от 25 мая 2017 года № 2017/11

О присуждении Маркину Юрию Витальевичу, гражданину РФ ученой степени кандидата технических наук.

Диссертация «Методы и средства углубленного анализа сетевого трафика» по специальности 05.13.11 – «математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей» принята к защите 24 марта 2017 г., протокол № 2017/07 диссертационным советом Д 002.087.01 на базе Федерального государственного бюджетного учреждения науки Институт системного программирования 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 Маркин Юрий Витальевич, 1989 года рождения, работает младшим научным сотрудником в Федеральном государственном бюджетном учреждении науки Институт системного программирования Российской академии наук.

В 2012 году соискатель с отличием окончил Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (государственный университет)» (МФТИ). В 2015 году соискатель окончил очную аспирантуру МФТИ.

Диссертация выполнена в Федеральном государственном бюджетном учреждении науки Институт системного программирования Российской

академии наук (ведомственная принадлежность – Федеральное агентство научных организаций), адрес: 109004, г. Москва, ул. А. Солженицына, дом 25, в отделе компиляторных технологий.

Научный руководитель – кандидат физико-математических наук Падарян Вартан Андроникович, ведущий научный сотрудник в Федеральном государственном бюджетном учреждении науки Институт системного программирования Российской академии наук, отдел компиляторных технологий.

Официальные оппоненты:

1. Гергель Виктор Павлович, доктор технических наук, профессор, директор Института информационных технологий, математики и механики Нижегородского государственного университета имени Н.И. Лобачевского, зав. кафедрой Программной инженерии,
2. Волконский Владимир Юрьевич, кандидат технических наук, старший научный сотрудник, начальник отделения "Системы программирования" публичного акционерного общества "ИНЭУМ им. И.С. Брука"

дали положительные отзывы на диссертацию.

Ведущая организация Федеральный исследовательский центр «Информатика и управление» Российской академии наук (г. Москва) в своем положительном заключении, подписанном ученым секретарем ФИЦ ИУ РАН, доктором технических наук В.Н. Захаровым, заведующим отделом ФИЦ ИУ РАН, доктором физико-математических наук, профессором В.А. Серебряковым, главным научным сотрудником ФИЦ ИУ РАН, доктором технических наук, профессором И.Н. Синициным, указала, что диссертация Маркина Ю.В. является законченной научно-квалифицированной работой, в которой содержится разработка методического и инструментального программного обеспечения углубленного анализа сетевого трафика в помехоустойчивых перспективных информационных системах высокой доступности, позволяющих автоматизировать расширение их функциональности. Диссертация Маркина Ю.В. соответствует требованиям, предъявляемым к диссертациям на соискание

ученой степени кандидата наук по специальности 05.13.11 «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей». Ее автор, Маркин Юрий Витальевич заслуживает присуждения ему искомой ученой степени кандидата технических наук по специальности 05.13.11.

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 9 опубликованных работ, из них 7 работ по теме диссертации, в том числе 4 статьи опубликованы в рецензируемых научных изданиях.

Публикации посвящены выявлению ограничений существующих анализаторов сетевого трафика, способам увеличения глубины разбора сетевых пакетов, представлению результатов разбора сетевого трафика, разработке архитектуры для инструментов анализа сетевого трафика.

Наиболее значимые научные работы по теме диссертации опубликованы в статьях:

1. A.I. Get’man, V.P. Ivannikov, Yu.V. Markin, V.A. Padaryan, A.Yu. Tikhonov. Data representation model for in-depth analysis of network traffic. // Programming and Computer Software, Volume 42, Issue 5, 2016, pp 316-323.
2. А.И. Гетьман, Ю.В. Маркин, Д.О. Обыденков, В.А. Падарян, А.Ю. Тихонов. Подходы к представлению результатов анализа сетевого трафика. // Труды Института системного программирования РАН, том 28, выпуск 6, 2016, стр. 103-110.
3. Ю.В. Маркин, В.А. Падарян, А.Ю. Тихонов. Программная инфраструктура для глубокого анализа сетевого трафика. // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». Санкт-Петербург, 29 июня - 02 июля 2015. Стр. 87-89

4. Ю.В. Маркин, В.А. Падарян, А.Ю. Тихонов. Ограничения современных программных средств глубокого анализа сетевого трафика и способы их преодоления. // Материалы 58-й научной конференции МФТИ. Москва–Долгопрудный–Жуковский, 23 - 28 ноября 2015 г.

Диссертационный совет отмечает, что в процессе выполнения работы соискателем:

- разработана модель представления сетевых данных, позволяющая учитывать:
  - потерю и переупорядочивание пакетов,
  - сжатие и шифрование данных,
  - присутствие пакетов различных протоколов на одном и том же уровне сетевого стека.
- для протоколов произвольного уровня сетевого стека разработан алгоритм сборки потоков данных для случаев изменения порядка пакетов при передаче;
- разработана архитектура системы анализа сетевого трафика, позволяющая автоматизировать создание и отладку разборщиков пакетов сетевых протоколов на предварительно сохраненном трафике для последующего использования их при разборе трафика на потоке;
- реализованы инструменты для проведения разбора сетевого трафика в online и offline режимах.

Теоретическая значимость исследования состоит в том, что:

- разработана модель представления сетевых данных, позволяющая разделять и выполнять независимо фазы распознавания и разбора пакетов протоколов произвольного сетевого стека, а также идентифицировать логические соединения и получать доступ к данным этих соединений;
- разработан алгоритм сборки потоков данных, обладающий устойчивостью к изменению порядка пакетов при передаче;
- разработана архитектура системы анализа трафика, позволяющая использовать один и тот же набор исходных кодов программ разборщиков для проведения разбора пакетов в online и offline режимах.

Значение полученных соискателем результатов исследования для практики состоит в том, что:

- на базе предложенных автором модели, алгоритма и архитектуры системы анализа трафика были разработаны и реализованы инструменты для проведения разбора сетевого трафика в online и offline режимах;
- Online-анализатор предназначен для использования сторонними системами посредством API для получения результатов разбора сетевого трафика;
- Offline-анализатор используется для создания разборщиков пакетов сетевых протоколов в разработанной системе анализа сетевого трафика, при решении задач, связанных с обратной инженерией или отладкой сетевых протоколов, в области научных исследований и в учебных курсах ВМК МГУ и ФУПМ МФТИ.

Достоверность результатов исследования состоит в том, что:

- экспериментальные результаты для оценки возможности разбора пакетов протоколов произвольного сетевого стека получены на файлах с трафиком, опубликованных в открытом доступе на официальном сайте анализатора Wireshark, а также интернет ресурсе PacketLife;
- для файлов с трафиком, в которых изменен порядок пакетов при передаче, разработанная система разбора сетевого трафика позволила увеличить глубину разбора пакетов по сравнению с рассмотренными в обзоре инструментами анализа сетевого трафика;
- в частных случаях установлено качественное и количественное совпадение авторских результатов с результатами, представленными в независимых источниках по данной тематике.

Личный вклад соискателя состоит в разработке модели представления сетевых данных, разработке алгоритма сборки потоков данных, разработке архитектуры системы анализа сетевого трафика, реализации инструментов для проведения разбора пакетов в online и offline режимах. В публикациях по выполненной работе автору принадлежат предложенные в них подходы к

анализу сетевого трафика, обзорная часть по существующим сетевым анализатором, экспериментальные оценки качества разбора сетевого трафика, проводимого рассмотренными в обзоре инструментами.

На заседании 25 мая 2017 года диссертационный совет принял решение присудить Маркину Ю.В. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 14 человек, из них 6 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 20 человек, входящих в состав совета, проголосовали: за – 14, против – 0, недействительных бюллетеней – 0.

Председатель диссертационного совета,
член-корр. РАН Аветисян А. И.

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

25 мая 2017 г.