# ОТЗЫВ

на автореферат диссертации Салахутдиновой Ксении Иркиновны на тему «Методика идентификации исполняемых файлов на основе статического анализа характеристик дизассемблированного кода программ», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Использование открытого программного обеспечения в локальных сетях организаций, определяет область исследования, связанную с разработкой интеллектуальных технологий для обеспечения автоматизированного процесса проведения аудита носителей информации посредством идентификации исполняемых файлов на основе присущих им уникальных характеристик. Актуальной научно-технической задачей является повышение эффективности организации комплексного обеспечения информационной безопасности и поддержание требуемого уровня защищенности обрабатываемой, хранимой и передаваемой информации.

Предметом диссертационного исследования, направленного на решение отмеченной задачи, являются методы идентификации программного обеспечения на основе статического анализа характеристик дизассемблированного кода программ. В диссертационном исследовании развиваются научные основы разработки систем активного мониторинга конечных узлов внутренней сети для поддержания мер по защите информации.

Представленные в автореферате результаты обладают требуемой для кандидатской диссертации научной новизной. Получены новые методы идентификации (формирования и сравнения сигнатур) исполняемых файлов, позволяющие (за счет автоматизации процесса) снизить трудозатраты на поиск и распознавание программного обеспечения. Предложена методика идентификации ПО, которая позволяет производить сравнение набора характеристик рассматриваемой программы с набором характеристик эталонной программы, за счет использования уникального устойчивого признакового пространства, машинного обучения и теории полезности.

Достоверность научных положений, результатов и выводов диссертационной работы обеспечивается за счет выполненного анализа многочисленных публикаций в области идентификации программного

обеспечения. Полученные результаты согласуются с уже известными решениями, не противоречат им. Теоретические выводы согласуются с результатами проведенного экспериментального исследования. Качество разработанной методики оценивается на основе исследования экспериментальных образцов исполняемых файлов.

Положения диссертации отражены в научных работах автора: опубликовано 32 научные работы и приравненных к ним публикаций, среди которых 8 работ в международных изданиях, индексируемых в реферативных базах Web of Science и Scopus, и 8 работ в журналах из списка ВАК. Получено 6 свидетельств о государственной регистрации программ для ЭВМ. Основные результаты диссертации были представлены на международных и российских научных мероприятиях.

Практическая значимость работы заключается в том, что полученные результаты используются для развития систем аудита персональных компьютеров пользователей и подключенных к локальной сети электронных носителей информации.

Положительно оценивая результаты, представленные в автореферате, необходимо отметить, что работа не лишена недостатков. Выделим следующие.

1. В качестве основной предметной области для практического применения полученных результатов выступает локальная сеть организации. При этом, отсутствие иллюстрирующих примеров в тексте автореферата затрудняет анализ представленных в нем теоретических положений.

2. Представляется, что при проведении мониторинга автоматизированной сети необходимо учитывать возможности используемой вычислительной и сетевой аппаратно-программной базы. В тоже время, в описании предложенной методики идентификации ПО в тексте автореферата этот вопрос не рассматривается.

3. В работе не рассмотрены проблемы информационной безопасности, которые безусловно возникают при анализе легитимных исполняемых файлов с внедренным вредоносным кодом или дополнительным функционалом.

Содержание автореферата свидетельствует о том, что диссертация представляет собой законченную научно-квалификационную работу, результаты получены лично автором и решают важную научно-техническую задачу по развитию методологических основ идентификации не вредоносного

программного обеспечения с использованием методов, не основанных на проверке метаданных и целостности данных программного кода.

Обобщая высказанное, считаю, что представленная к защите диссертационная работа соответствует всем требованиям «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства РФ от 24.09.2013 г. № 842 и предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, а ее автор, Салахутдинова Ксения Иркиновна, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Доцент кафедры информатики и математического обеспечения
института математики и информационных технологий ПетрГУ,
кандидат физико-математических наук,
доцент

«17» января 2020 г. Корзун Д.Ж.

**Сведения о составителе отзыва:**

*Фамилия, Имя, Отчество*: Корзун Дмитрий Жоржевич
*Ученая степень*: кандидат физико-математических наук
*Ученое звание:* доцент
*Место работы*: Федеральное государственное бюджетное образовательное учреждение высшего образования Петрозаводский государственный университет (ПетрГУ)
*Должность*: доцент кафедры информатики и математического обеспечения, институт математики и информационных технологий
*Почтовый адрес*: 185910, Республика Карелия, г. Петрозаводск, пр. Ленина, 33
*Телефон*: +7 (8142) 711084
*E-mail*: dkorzun@cs.karelia.ru

Корзуна Д.Ж.
ЗАВЕРЯЮ
ИСТ
РАМ
Тришина Е.Ю.
«17» 01 2020 г.