ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.199.01, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ НАУКИ САНКТ-ПЕТЕРБУРГСКОГО ИНСТИТУТА ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ РОССИЙСКОЙ АКАДЕМИИ НАУК МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 18.02.2020 г. № 2

О присуждении Салахутдиновой Ксении Иркиновне, гражданке Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Методика идентификации исполняемых файлов на основе статического анализа характеристик дизассемблированного кода программ» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 10 декабря 2019 г., протокол № 2 диссертационным советом Д 002.199.01, созданным на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, Министерства науки и высшего образования Российской Федерации, 199178, Россия, Санкт-Петербург, 14 линия ВО, дом 39, утвержден приказом Рособрнадзора номер 2472-618 от 8 октября 2010 года (с изменениями согласно приказам Минобрнауки России №105/нк от 11 апреля 2012 г. №574/нк от 15 октября 2014 г., № 386/нк от 27 апреля 2017 г., №748/нк от 12 июля 2017 г., №301/нк от 23 ноября 2018 г.).

Соискатель Салахутдинова Ксения Иркиновна, 1994 года рождения, в 2017 г. с отличием окончила федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» по направлению подготовки 10.04.01 – «Информационная безопасность» (диплом № 107824 1782536 выдан 30 июня 2017 года). Справка об обучении №44/2019, выдана федеральным государственным автономным образовательным учреждением высшего образования «Санкт-Петербургский национальный исследовательский университет

информационных технологий, механики и оптики». В настоящее время Салахутдинова Ксения Иркиновна работает младшим научным сотрудником в лаборатории интеллектуальных систем Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, Министерства науки и высшего образования Российской Федерации.

Диссертация выполнена в лаборатории интеллектуальных систем Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, Министерства науки и высшего образования Российской Федерации.

Научный руководитель – доктор технических наук, профессор ЛЕБЕДЕВ Илья Сергеевич, основное место работы: Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), главный научный сотрудник лаборатории интеллектуальных систем.

Официальные оппоненты:

БУРЛОВ Вячеслав Георгиевич, доктор технических наук, профессор, профессор кафедры информационных технологий и систем безопасности Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный гидрометеорологический университет»;

ПРИМАКИН Алексей Иванович, доктор технических наук, профессор, начальник кафедры специальных информационных технологий Федерального государственного казенного образовательного учреждения высшего образования «Санкт-Петербургского университета Министерства внутренних дел Российской Федерации» дали положительные отзывы на диссертацию.

Ведущая организация – Федеральное государственное бюджетное образовательное учреждение высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова», г. Санкт-Петербург в своем положительном отзыве, подписанном Соколовым Сергеем Сергеевичем, д.т.н., доцентом, заведующим кафедрой комплексного обеспечения информационной безопасности ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова», и утвержденном ректором д.т.н., профессором Барышниковым С.О., указала, что диссертационное

исследование К.И. Салахутдиновой представляет собой завершенную научно-исследовательскую работу, выполненную на актуальную тему, отличается научной новизной и практической значимостью полученных результатов. Автором в диссертации сформулирована и решена важная научно-техническая задача разработки и обоснования научно-методического аппарата идентификации исполняемых файлов, устанавливаемых на средства вычислительной техники, обеспечивающего увеличение точности идентификации в условиях наличия различных версий, большого числа различных наименований программ и ограниченности числа объектов обучающей выборки.

Соискателем предложен метод формирования сигнатур исполняемых файлов, отличающийся от существующих использованием ряда отобранных наиболее информативных и устойчивых в проявлении ассемблерных команд. Предложен метод сравнения сигнатур идентифицируемых исполняемых файлов с ранее сформированными эталонными сигнатурами программ, отличающийся от известных применением комбинированного подхода использования алгоритма машинного обучения и аддитивного критерия. Разработана методика идентификации программ, отличающаяся от известных применением уникального сформированного признакового пространства и теории полезности для принятия решения на основе аддитивного критерия. Полученные в диссертационной работе научные результаты, выводы и практические рекомендации могут найти применение в различных проектах при разработке систем защиты информации, аудита электронных носителей информации, функционирующих в организациях МО РФ, МВД РФ, РАН, СПбФ ФО «НПК ТРИСТАН», АО «ЭВРИКА» и промышленности, а также в действующих организациях, реализующих основные направления задач мониторинга информационной безопасности. Текст автореферата полностью соответствует содержанию диссертации. Диссертационное исследование «Методика идентификации исполняемых файлов на основе статического анализа характеристик дизассемблированного кода программ» является научно-квалификационной работой и соответствует критериям, изложенным в пп. 9-14 «Положения о присуждении ученых степеней», утвержденного постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 г., предъявляемых к кандидатским диссертациям, а его автор Салахутдинова Ксения Иркиновна заслуживает присуждения ученой степени

кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Соискатель имеет 32 опубликованных работы, все по теме диссертации, в том числе опубликованных в рецензируемых научных изданиях 16 работ, из них опубликованных в изданиях, рекомендуемых ВАК при Минобрнауки России – 8 работ, в изданиях, индексируемых в базах данных Scopus и Web of Science – 8; получено 6 свидетельств о государственной регистрации программ для ЭВМ.

Основные научные результаты опубликованы в 26 научных трудах общим объемом 10,46 п.л., из которых 16 статей в журналах объемом 8,46 п.л., выполнены в соавторстве, а 1 статья объемом 0,75 п.л. – лично. Наиболее значимые работы по теме диссертации:

1. **Салахутдинова К.И.** Повышение точности идентификации программного обеспечения путем использования аддитивного критерия Фишберна // Информационные технологии - 2019. - Т. 25. - № 10. - С. 609–614. (Перечень ВАК)
2. **Салахутдинова К.И.**, Малков В.В., Кривцова И.Е. Сравнительный анализ подходов к идентификации программного обеспечения // Безопасность информационных технологий - 2019. - Т. 26. - № 2. - С. 58-66. (Перечень ВАК). *Личный вклад соискателя – 33%.*
3. **Салахутдинова К.И.**, Лебедев И.С., Кривцова И.Е. Подход к выбору информативного признака в задаче идентификации программного обеспечения // Научно-технический вестник информационных технологий, механики и оптики - 2018. - Т. 18. - № 2(114). - С. 278–285. (Перечень ВАК). *Личный вклад соискателя – 33%.*
4. **Salakhutdinova K.I.**, Krivtsova I.E., Lebedev I.S., Sukhoparov M.E. An Approach to Selecting an Informative Feature in Software Identification // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) - 2018, Vol. 11118, pp. 318-327. (База данных Scopus). *Личный вклад соискателя – 30%.*
5. **Salakhutdinova K.I.**, Lebedev I.S., Krivtsova I.E., Sukhoparov M.E. Studying the Effect of Selection of the Sign and Ratio in the Formation of a Signature in a Program Identification Problem // Automatic Control and Computer Sciences - 2018, Vol. 52, No. 8, pp. 1101–1104. (База данных Scopus). *Личный вклад соискателя – 30%.*

6. **Salakhutdinova K.I.**, Krivtsova I.E., Lebedev I.S. Identification of Executable Files on the basis of Statistical Criteria // Proceedings of the 20th Conference of Open Innovations Association FRUCT - 2017, pp. 202-208. (База данных Scopus). *Личный вклад соискателя – 33%.*

Оригинальность содержания диссертации составляет не менее 90% от общего объёма текста; цитирование оформлено корректно; заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем учёной степени в соавторстве без ссылок на соавторов не выявлено. Недостоверные сведения об опубликованных соискателем ученой степени работах в диссертации отсутствуют.

На автореферат диссертации поступило 10 отзывов, все отзывы положительны:

1) Санкт-Петербургский филиал ФГБУ науки Института земного магнетизма, ионосферы и распространения радиоволн им. Н.В. Пушкова Российской академии наук. Отзыв составил заместитель директора по науке, д.т.н., профессор Коробейников Анатолий Григорьевич. Замечания: В автореферате перечислены компьютерные программы, разработанные в процессе исследования, однако не упоминается возможность создания комплексного программного продукта, представляющего собой самостоятельный блок автоматического мониторинга средств вычислительной техники. На странице 3 автореферата, говорится: «Возможные дефекты программного обеспечения … могут привести к росту числа уязвимостей и повлиять на информационную безопасность систем» однако отсутствует описание возможных уязвимостей и способов их эксплуатации.

2) ФГБОУ ВПО «Санкт-Петербургский государственный университет». Отзыв составил профессор кафедры информационных систем в экономике, д.ф.-м.н., профессор Юрков Александр Васильевич. Замечания: В тексте не предоставлены используемые модели нарушителя и угроз. Не четко обозначены границы применимости разработанной методики. Нет пояснений для коэффициентов в формуле на стр. 14.

3) ФГАОУ ВО «Северный (Арктический) федеральный университет имени М.В. Ломоносова». Отзыв составил заведующий кафедрой Информатики и информационной безопасности, к.т.н., доцент Василишин Игорь Иванович. Замечания:

В описании четвертой главы отсутствует информация о характеристиках рассматриваемых исполняемых файлах, что не дает возможность получить представление о проведенных экспериментальных исследованиях. В работе рассматриваются исполняемые файлы формата ELF, однако не говорится о том, возможно ли применение разработанной методики к исполняемым файлам других форматов, например, PE.

4) ФАС ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича». Отзыв составил доцент кафедры Безопасности информационных систем, к.ф.-м.н. доцент, Кривцов Александр Николаевич. Замечания: В автореферате приводятся результаты трех способов оценки точности идентификации: матрица ошибок (Confusion Matrix), точности (Accuracy), бикубической меры (F-measure), однако из текста автореферата не ясна причина выбора такого числа и именно таких способов оценки. В автореферате приводятся результаты проведенных экспериментов с целью проверки достигаемой точности идентификации при помощи разработанной методики, однако отсутствует описание рассматриваемой выборки: ее объем, функциональная направленность программ, число различных версий, способ дизассемблирования и т.п.

5) ФГБОУ ВО «Петрозаводский государственный университет». Отзыв составил доцент кафедры информатики и математического обеспечения, к.ф.-м.н., доцент Корзун Дмитрий Жоржевич. Замечания: 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. Представляется, что при проведении мониторинга автоматизированной сети необходимо учитывать возможности используемой вычислительной и сетевой аппаратно-программной базы. В то же время, в описании предложенной методики идентификации ПО в тексте автореферата этот вопрос не рассматривается. В работе не рассмотрены проблемы информационной безопасности, которые безусловно возникают при анализе легитимных исполняемых файлов с внедренным вредоносным кодом или дополнительным функционалом.

6) ФГАОУ ВО «Национальный исследовательский университет «Высшая школа экономики». Отзыв составил руководитель департамента логистики и управления цепями поставок, заслуженный деятель науки РФ, д.т.н., профессор, Лукинский Валерий Сергеевич. Замечания: На с. 8 говорится, что «…которая при помощи заданного алгоритма и выбранной характеристики F формирует частотную последовательность признака версии программы…» однако не ясно, что является характеристикой F. На с. 8 говорится, что «Требовалось построить алгоритм… при условии ограничений на: … не способность классификации выдать корректный результат для программы, класс которой не был определен на этапе формирования модели классификации (нельзя создать класс «файл не похож ни на одну из программ»)». Однако неясно, каким именно способом преодолевается данное ограничение. На с.11 говорится, что «Приводится три способа оценки точности идентификации…», однако не сказано, чем вызвано такое разнообразие. Из текста автореферата не до конца понятно, какую структуру имеет сигнатура исполняемого файла и каким образом происходит итерационный процесс идентификации. Сигнатура состоит из непрерывной последовательности распределений по каждому отобранному признаку и рассматривается как единое целое, или представляет собой набор индивидуальных распределений по каждому отобранному признаку, анализируемых поочередно.

7) АО «НПП «ИСТА-Системс». Отзыв составил ведущий инженер, к.т.н. Кукунин Дмитрий Сергеевич. Замечания: Недостаточно полное раскрытие вопроса эффективности существующих методов идентификации программного обеспечения, основанных на машинном обучении при рассматриваемых условиях. Недостаточно подробный анализ вычислительной сложности предлагаемых алгоритмов выявления встроенных сообщений.

8) Санкт-Петербургский филиал АО «НПК «ТРИСТАН». Отзыв составил заместитель директора по программному обеспечению, к.т.н., Шахпаронян Артем Павлович. Замечания: Остается не до конца ясным на основе какого принципа происходит выбор конкретных ассемблерных команд и какое число ассемблерных команд участвует в анализе их информативности. В тексте автореферата упоминается тестирование различных алгоритмов машинного обучения и статистических

критериев, однако не вполне ясно, учитывается ли вычислительная сложность алгоритмов при их оценке эффективности.

9) ООО «АПСТЭК Лабс». Отзыв составил инженер-программист 1ой категории, к.т.н. Спивак Антон Игоревич. Замечания: Из автореферата неясно, по какому принципу присутствует цветовое выделение элементов в приведенном графическом представлении методики идентификации на рисунке 1. Качество иллюстрированного материала, а именно размер графиков а) и б) на рисунке 5, не способствуют облегчению восприятия материала.

10) ООО «Цезурити». Отзыв составил руководитель проектов, к.т.н. Лапшин Сергей Владимирович. Замечания: наличие некоторых стилистических погрешностей в тексте, а также описание предложенной методики идентификации исполняемых файлов представлено автором слишком кратко.

Выбор официальных оппонентов и ведущей организации обосновывается тем, что

доктор технических наук, профессор Бурлов Вячеслав Георгиевич является известным ученым в области защиты информации и обеспечения безопасности автоматизированных систем;

доктор технических наук, профессор Примакин Алексей Иванович – известный специалист в области обеспечения безопасности в сетях обработки документов ограниченного доступа;

ведущая организация, Федеральное государственное бюджетное образовательное учреждение высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова», является известной как в России, так и за рубежом организацией в области разработки и исследований систем защиты информации, составляющей, в том числе, государственную тайну.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработаны новые алгоритмы, методы и методика идентификации исполняемых файлов, устанавливаемых на средства вычислительной техники, обеспечивающие увеличение точности в условиях наличия различных версий, большого числа наименований программ и ограниченности числа объектов обучающей выборки;

предложены:

– метод формирования сигнатур исполняемых файлов, основанный на построении частотного распределения каждой из градаций выделенной характеристики исполняемых файлов, отличающийся от существующих использованием ряда отобранных наиболее информативных и устойчивых в проявлении ассемблерных команд и обеспечивающий создание уникальных по форме и амплитуде частотных распределений.

– метод сравнения сигнатур идентифицируемых исполняемых файлов с ранее сформированными эталонными сигнатурами программ, отличающийся от известных применением комбинированного подхода на основе использования алгоритма машинного обучения и аддитивного критерия, способствующего снижению числа ошибочных результатов классификации и обеспечивающего увеличение точности от совокупного использования признакового пространства, а также учитывающего ряд изменений в коде исполняемых файлов, что позволяет максимизировать эмерджентность совокупности признакового пространства и идентифицировать не рассматриваемые на этапе обучения версии программ;

– методика идентификации программного обеспечения, основанная на комбинированном анализе характеристик дизассемблированного кода программ, отличающаяся от известных применением уникального сформированного признакового пространства и теории полезности для принятия решения на основе аддитивного критерия при комбинированном анализе характеристик из их дизассемблированного представления и обеспечивающая увеличение точности идентификации версий программ, ранее не задействованных в создании эталонных сигнатур исполняемых файлов;

– практические рекомендации по применению разработанного научно-методического аппарата, включающие в себя указания по формированию архива сигнатур, а также по применению метода и методики идентификации исполняемых файлов, позволяющих обнаруживать нарушения установленных мер политики безопасности в плане запрета на несанкционированную установку программного обеспечения;

доказана:

– возможность идентификации исполняемых файлов ELF формата на наборе признаков, характеризующих дизассемблерный код представления программы;

– перспективность использования предложенного научно-методического аппарата для построения систем детектирования и распознавания исполняемых файлов на основе статического анализа характеристик их дизассемблированного кода;

введены:

– сигнатурное представление исполняемых файлов для различных видов программного обеспечения, которое характеризуется определенными величинами признаков, рассредоточенными в коде представления программы на низкоуровневом языке программирования;

– требования к процессу идентификации исполняемых файлов на электронных носителях информации, связанные с существованием большого числа различных наименований программ и ограниченности числа объектов обучающей выборки.

Теоретическая значимость исследования обоснована тем, что:

доказаны сформулированные в работе теоретические утверждения с использованием формальных математических доказательств и серией вычислительных экспериментов о применимости предложенных методов и методики. Эти утверждения составляют основу процесса идентификации исполняемых файлов на электронных носителях информации с целью обеспечения конфиденциальности и целостности информации, обрабатываемой в автоматизированной системе;

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов)

использованы теория информационной безопасности, методы математической статистики, теория предпочтений, методы машинного обучения, экспериментальные методы исследования;

изложены методологические и методические основы использования математического аппарата статистического анализа для формирования индивидуальных характеристических последовательностей исполняемых файлов;

раскрыты

проблемные аспекты применения имеющихся подходов в области обеспечения информационной безопасности и идентификации установленного программного обеспечения в следствии наличия ряда ограничений и недостаточных возможностей по обеспечению комплексной реализации мер по информационной безопасности;

основные вопросы, связанные с несанкционированно установленным программным обеспечением, при котором образуется потенциальная возможность возникновения новых уязвимостей в автоматизированной системе, эксплуатация которых может быть направлена на конфиденциальность и целостность информации;

аспекты, обусловленные универсальностью и практической применимостью предложенных методов и методики идентификации исполняемых файлов при ограниченном числе объектов обучающей выборки;

изучены существующие концепции, стандарты, технологии, программные средства, модели и методы идентификации исполняемых файлов в автоматизированных системах, при этом особое внимание уделено идентификации не вредоносных программ различного назначения и функциональности; существующие методы интеллектуального анализа данных и особенности совместного применения различных алгоритмов машинного обучения в задачах многоклассовой классификации;

проведена модернизация существующих подходов к идентификации исполняемых файлов, установленных на электронных носителях информации; метода и методики идентификации при использовании анализа характеристик дизассемблированного кода программ.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработаны и внедрены (указать степень внедрения) следующие результаты диссертационной работы:

– метод формирования эталонных сигнатур программ и идентифицируемых исполняемых файлов, основанный на статическом подходе анализа характеристик дизассемблированных кодов программ – внедрен в рамках научно-исследовательской

работы, выполненной в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН) – проект по программе Президиума РАН № 0073- 2018-0008 «Теория и распределенные алгоритмы самоорганизации группового поведения агентов в автономной миссии», 2018,2019гг.; в образовательном процессе факультета БИТ Университета ИТМО по направлениям подготовки бакалавриата 10.03.01 и магистратуры 10.04.01 по дисциплинам «Организация и управление службой защиты информации», «Теория вероятностей», «Методы цифровой обработки видеоизображений», «Управление информационной безопасностью»;

– метод сравнения сигнатур идентифицируемых исполняемых файлов с ранее сформированными эталонными сигнатурами программ при помощи комбинированного подхода использования алгоритма машинного обучения – градиентного бустинга деревьев решений и аддитивного критерия Фишберна, позволяющий достигать наименьшего числа ошибок неверной классификации и максимизировать эмерджентность совокупности признакового пространства – внедрен в рамках научно-исследовательской работы, выполненной в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН) – проект по программе Президиума РАН № 0073- 2018-0008 «Теория и распределенные алгоритмы самоорганизации группового поведения агентов в автономной миссии», 2018,2019гг.; в образовательном процессе факультета БИТ Университета ИТМО по направлениям подготовки бакалавриата 10.03.01 и магистратуры 10.04.01 по дисциплинам «Организация и управление службой защиты информации», «Теория вероятностей», «Методы цифровой обработки видеоизображений», «Управление информационной безопасностью»;

– методика идентификации исполняемых файлов, включающая разработанные методы по формированию и сравнению сигнатур идентифицируемых исполняемых файлов с эталонными сигнатурами программ – внедрена при разработке системы мониторинга состояния внутренних сетей компании АО «НПК «ТРИСТАН»;

определены возможности и перспективы практического использования полученных результатов диссертации при разработке системы обнаружения

несанкционированно установленного программного обеспечения в целях повышения безопасности информационной системы организации;

создано модельно-алгоритмическое и программное обеспечение, представляющее собой основу для разработки системы обнаружения и предотвращения несанкционированной установки программного обеспечения на основе статического анализа характеристик дизассемблированного кода программ, увеличивающего точность идентификации исполняемых файлов, и позволяющее устранить недостатки существующих методов;

представлены предложения и направления для дальнейших научных исследований, в основу которых могут быть положены разработанные методы и методика.

Оценка достоверности результатов исследования выявила:

для экспериментальных работ результаты получены на проверенном вычислительном оборудовании, показана воспроизводимость результатов исследования, сделанные выводы подтверждены результатами анализа собранных данных с использованием современных программных средств;

достоверность полученных результатов подтверждена проведением всестороннего анализа работ по исследуемой проблеме, корректным применением научно-методического аппарата в виде использованных методов и теорий, апробацией основных результатов диссертации в печатных трудах и докладах на международных и всероссийских конференциях, положительными итогами практической реализации результатов работы;

теория построена на известных принципах, проверенных данных и фактах с использованием современных апробированных методов информационной безопасности и методологии защиты информации, методов математической статистики, теории предпочтений, методов машинного обучения, экспериментальных методов исследования, согласуется с опубликованными частными результатами других исследователей;

идея базируется на анализе работ отечественных и зарубежных исследователей в области идентификации исполняемых файлов и обеспечении информационной безопасности автоматизированных систем;

использованы полученные характеристики модели представления исполняемых файлов и метода их идентификации для сравнения с данными, приведенными в современной научной литературе по обнаружению и предотвращению несанкционированной установки программного обеспечения;

установлено качественное и количественное соответствие результатов решения задачи разработки методов и методики идентификации исполняемых файлов на основе статического анализа набора признаков, характеризующих отличительные особенности различных программ. При этом подтверждено преимущество предложенного подхода перед результатами, полученными другими авторами.

использованы современные методики сбора и обработки исходной информации, теория информационной безопасности, методы математической статистики, теория предпочтений, методы машинного обучения, экспериментальные методы исследования.

Личный вклад соискателя состоит в:

– анализе современного состояния исследований в области идентификации исполняемых файлов не вредоносного характера;

– постановке задачи разработки научно-методического аппарата по идентификации исполняемых файлов;

– обосновании выбора показателей эффективности идентификации исполняемых файлов, таких как точность, бикубическая мера, матрица неточностей, количество идентификационных признаков;

– разработке и обосновании модели представления программного обеспечения на основе выделенной комбинации наиболее информативных признаков;

– разработке и обосновании метода формирования эталонных сигнатур программ и сигнатур идентифицируемых исполняемых файлов на основе статического подхода анализа характеристик дизассемблированных кодов программ;

– разработке и обосновании метода идентификации исполняемых файлов на основе комбинированного подхода использования алгоритма машинного обучения – градиентного бустинга деревьев решений и аддитивного критерия Фишберна;

– разработке и обосновании методики идентификации исполняемых файлов;

– анализе применимости предложенных методов и методики при накладываемых ограничениях на потенциальное количество различных программ и их версий, на наличие существенных изменений в их коде;

– разработке практических рекомендаций по применению предложенного научно-методического аппарата;

– подготовке основных публикаций по выполненной работе.

Диссертационный совет считает, что Салахутдинова К.И. в своей диссертационной работе решила научную задачу разработки и обоснования научно-методического аппарата по идентификации исполняемых файлов, устанавливаемых на средства вычислительной техники, обеспечивающего увеличение точности идентификации в условиях наличия различных версий, большого числа различных наименований программ и ограниченности числа объектов обучающей выборки, имеющую важное социально-экономическое и хозяйственное значение в области информационных технологий и безопасности.

На заседании 18.02.2020 г. диссертационный совет принял решение присудить Салахутдиновой К.И. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 19 человек, из них 5 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за 19, против нет, недействительных бюллетеней нет.

Председатель диссертационного совета
доктор технических наук,
член-корреспондент РАН Юсупов Рафаэль Мидхатович

Ученый секретарь диссертационного совета
кандидат технических наук Зайцева Александра Алексеевна
18.02.2020 г.