ЗАКЛЮЧЕНИЕ

экспертной комиссии диссертационного совета Д.002.199.01 по кандидатской диссертации Салахутдиновой Ксении Иркиновны на тему: «Методика идентификации исполняемых файлов на основе статического анализа характеристик дизассемблированного кода программ», научный руководитель – д.т.н., профессор, заведующий лабораторией интеллектуальных систем СПИИРАН Лебедев И.С.

Экспертная комиссия диссертационного совета Д.002.199.01 в составе: д.т.н., проф. Саенко И.Б. (председатель), д.т.н., проф. Осипов В.Ю, д.т.н., проф. Молдовян Н.А. после ознакомления с кандидатской диссертацией Салахутдиновой Ксении Иркиновны на тему: «Методика идентификации исполняемых файлов на основе статического анализа характеристик дизассемблированного кода программ» сделала вывод о том, что диссертационная работа Салахутдиновой К.И. посвящена решению актуальной научной задачи: разработке и обосновании научно-методического аппарата по идентификации исполняемых файлов, устанавливаемых на средства вычислительной техники, обеспечивающего максимальную точность идентификации в условии наличия различных версий программного обеспечения, большого числа различных наименований программ и ограниченности числа объектов обучающей выборки, обусловленное реальным состоянием выпускаемых версий того или иного программного обеспечения.

Целью исследования является увеличение точности идентификации установленного ПО при заданных ограничениях и автоматизация аудита электронных носителей информации. Противоречие, возникающее между недостаточной точностью идентификации ПО существующими методами и необходимостью по обеспечению достаточного уровня защищенности информации в информационной системе, обуславливает актуальность данного исследования.

Практическую значимость исследования составляют разработанные в диссертации комплексный подход, методы и алгоритмы, которые обеспечивают решение актуальной научно-технической задачи, направленной на автоматизацию идентификации исполняемых файлов, и вносят значительный вклад в развитие инструментальной базы для проведения аудита электронных носителей информации. Результаты исследования внедрены в образовательном и научном учреждениях, коммерческом предприятии.

Интеграция математического аппарата и алгоритмов машинного обучения позволяет выявлять как структуру исполняемых файлов, так и распределение ее составляющих, учитывать технологические, конструктивные и эксплуатационные ограничения, что в конечном итоге служит основой для поддержки организационных и технических мер по запрету на несанкционированную установку программного обеспечения. На основе накопленных знаний о распределении признакового пространства дизассемблированных кодов объектов и их взаимосвязях, становится возможным выявление закономерностей присущих различным наименованиям программ.

Достоверность и обоснованность научных положений, основных выводов и результатов диссертации обеспечиваются использованием апробированного математического аппарата и подтверждается проведением сравнительного анализа с существующими методами; серией практических экспериментов по идентификации исполняемых файлов; проверкой адекватности положений и выводов; согласованностью результатов, полученных при теоретическом исследовании с результатами проведенных экспериментов; практической апробацией результатов исследования в докладах и публикациях на отечественных и зарубежных научных конференциях.

Материалы и основные результаты кандидатской диссертации Салахутдиновой К.И. удовлетворяют паспорту специальности: 05.13.19 – «Методы и системы защиты информации, информационная безопасность (технические науки)», по

которой диссертационному совету Д.002.199.01 предоставлено право проведения защит диссертаций.

Основные научные результаты диссертации удовлетворяют требованиям, предусмотренным пунктами 11 и 13 Положения о присуждении ученых степеней: по материалам диссертационной работы опубликовано 32 научных работ, в том числе 16 статей, из которых 8 статей в периодических журналах, рекомендованных ВАК (журналы «Научно-технический вестник информационных технологий, механики и оптики», «Проблемы информационной безопасности. Компьютерные системы», «Безопасность информационных технологий», «Авиакосмическое приборостроение», «Информационные технологии»).

Недостоверные сведения о работах, в которых изложены основные научные результаты диссертации, опубликованных соискателем ученой степени, отсутствуют.

Текст диссертации, представленной в диссертационный совет, идентичен тексту диссертации, размещенной на сайте СПИИРАН.

Объем оригинального текста диссертационной работы составляет не менее 90%; цитирование оформлено корректно. Требования, установленные пунктом 14 Положения о присуждении ученых степеней, соблюдены: заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем ученой степени в соавторстве, без ссылок на соавторов, не выявлено.

Комиссия предлагает:

1. Принять кандидатскую диссертацию Салахутдиновой К.И. к защите на диссертационном совете Д.002.199.01 как соответствующую профилю диссертационного совета по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность (технические науки)».
2. В качестве официальных оппонентов назначить специалистов по данной проблеме: д.т.н., проф. Бурлова В.Г., д.т.н., проф. Примакина А.И..
3. В качестве ведущей организации утвердить федеральное государственное бюджетное образовательное учреждение высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова» (ФГБОУ ВО ГУМРФ имени адмирала С.О. Макарова).
4. Разрешить Салахутдиновой К.И. опубликовать автореферат и утвердить список рассылки авторефератов.
5. Защиту диссертации назначить на «18» февраля 2020 г.

Члены комиссии: Саенко И.Б.

Осипов В.Ю.

Молдовян Н.А.