ОТЗЫВ

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

Поиск и распознавание программного обеспечения на компьютерах той или иной автоматизированной системы организации в настоящее время является достаточно актуальной задачей. Преодоление организационных мер, направленных на запрет по установке нелегитимного программного обеспечения на предприятии, приводит к формированию незарегистрированного потенциального источника уязвимостей, а, следовательно, снижает информационную безопасность всей системы в целом. Это еще раз подчеркивает актуальность задач, поставленных в диссертационной работе Салахутдиновой Ксении Иркиновны.

Диссертант предлагает использовать статический анализ характеристик дизассемблированного кода программ, заключающийся в построении информативной модели в виде математического кортежа по выбранному признаковому пространству, характеристики которой позволяют найти однозначное соответствие между анализируемой последовательностью и хранящимся эталоном исполняемого файла. Разработанные решения ориентированы специфично на случай идентификации исполняемых файлов не зависимо от их целостности, что особенно актуально в условиях популяризации гибкой методологии разработки программ, ускоряющих выпуск их новых версий.

Положительной стороной работы, исходя из автореферата, является высокая новизна предлагаемого подхода: задача увеличения точности идентификации исполняемых файлов именно при использовании комбинированного подхода машинного обучения и теории полезности для постобработки результатов мульти-классификации ранее не рассматривалась.

В качестве недостатков работы можно выделить следующие:

1. Недостаточно полное раскрытие вопроса эффективности существующих методов идентификации программного обеспечения, основанных на машинном обучении при рассматриваемых условиях.

2. Недостаточно подробный анализ вычислительной сложности предлагаемых алгоритмов выявления встроенных сообщений.

Несмотря на приведенные недостатки, диссертационная работа Салахутдиновой Ксении Иркиновны представляет собой законченную научно-квалификационную работу, выполненную на высоком уровне. Работа соответствует пунктам 9-14 «Положения о присуждении ученых степеней», утвержденного постановлением правительства Российской Федерации от 24 сентября 2013 года № 842 (в редакции от 01 октября 2018 года), предъявляемых к кандидатским диссертациям. Считаю, что Салахутдинова Ксения Иркиновна заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Ведущий инженер АО «НПП «ИСТА-Системс»
к.т.н.

«28» января 2020 г. ин

Сведения о составителе отзыва:
Фамилия, Имя, Отчество: Кукунин Дмитрий Сергеевич
Ученая степень: кандидат технических наук
Ученое звание:
Место работы: АО «НПП «ИСТА-Системс»
Должность: ведущий инженер
Почтовый адрес: 194100, Санкт-Петербург, ул. Харченко, д. 5, литер А
Телефон: +7-921-408-50-86
E-mail: coux@yandex.ru