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.

Развитие микроэлектронной базы и интернет-технологий привело к возрастанию доступности персональных компьютеров и интеграции компьютерных технологий на все уровни бизнес процессов предприятий. В доступном и большом количестве стали различные страницы сети Интернет, ориентированные на информирование интернет-пользователей о существующих уязвимостях операционных систем, программного обеспечения и эксплуатации нетривиальных способов обхода установленных на рабочих местах систем защиты информации. Таким образом, пользователь информационной системы способен стать потенциальным нарушителем информационной безопасности, и в частности, нарушить запрет на установку стороннего программного обеспечения.

Соискателем получен ряд новых научных и практических результатов, направленных на решение данной проблемы. Основными научными результатами автора являются:

1. Метод формирования эталонных сигнатур программ и сигнатур идентифицируемых исполняемых файлов.
2. Метод сравнения сигнатур идентифицируемых исполняемых файлов с ранее сформированными эталонными сигнатурами программ.
3. Методика идентификации исполняемых файлов.

Среди практических результатов необходимо отметить комплекс программных средств, направленных на автоматизацию процесса аудита электронных носителей информации.

По теме диссертационного исследования опубликовано 32 научных работы. Полученные результаты в достаточной степени апробированы на научных конференциях и подтверждены экспериментально.

Автореферат написан логично, хорошим научным языком. Вместе с тем, по содержанию автореферата имеется ряд вопросов и замечаний:

1. 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.

2. 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.

3. На с.11 говорится, что «Приводится три способа оценки точности идентификации…», однако не сказано, чем вызвано такое разнообразие.

4. 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.

Указанные вопросы, по-видимому, обусловлены ограниченным объемом автореферата и не снижают общего положительного впечатления от работы.

Проведенное диссертационное исследование характеризуется хорошей теоретической и экспериментальной проработкой предмета исследования. Содержание диссертации исчерпывающе отражено в научных публикациях

автора. Результаты диссертации обладают научной новизной и практической значимостью. Автореферат достаточно полно и точно отражает основные положения диссертации.

Считаю, что диссертационная работа на тему «Методика идентификации исполняемых файлов на основе статического анализа характеристик дизассемблированного кода программ» заслуживает высокой оценки, удовлетворяет 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».

Заслуженный деятель науки РФ,
доктор технических наук, профессор,
руководитель департамента логистики и управления цепями поставок
Санкт-Петербургского филиала ФГАОУ ВО «Национальный
исследовательский универс ла экономики»

Iукинский Валерий Сергеевич

«27» декабря

Санкт-Петербургский филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет «Высшая школа экономики»
194100, г. Санкт-Петербург, ул. Кантемировская, д. 3, корп. 1, лит. А
https://spb.hse.ru/
E-mail: vslukinskiy@hse.ru, телефон: +7 (812) 644-59-11 (+61517)

Под