ОТЗЫВ
на автореферат диссертации Ксении Иркиновны Салахутдиновой
«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»

Проблема информационной безопасности сегодня является одной из наиболее актуальных. Все чаще в СМИ встречаются упоминания о крупных инцидентах, связанных с нарушением конфиденциальности информации, повлекших за собой существенные последствия. Помимо этого, обострению ситуации в области информационной безопасности способствует напряженная обстановка в мире, которая проявляется в фактах вмешательства во внутренние политические процессы в том числе и посредством распространения некачественного программного обеспечения, которое, в частности, способно предоставить возможность для хакерских атак. Но угрозы информационной безопасности заключаются не только в производимых хакерских атаках, сами пользователи защищаемой автоматизированной системы способны оказывать деструктивное воздействие. При этом сейчас не нужно обладать техническими навыками высокого уровня, как правило, достаточно лишь уметь находить и устанавливать программное обеспечение на компьютер или портативную программу на съемный носитель.

Таким образом, проблема защиты автоматизированной системы от установки стороннего, нелегитимного программного обеспечения является актуальной. Решение данной проблемы предусматривает комплекс организационных и технических мер для предотвращения подобных инцидентов, а также анализ и мониторинг защищенности средств вычислительной техники на предмет возможности неправомерной установки программ. Диссертационная работа К.И. Салахутдиновой посвящена разработке методов представления и анализа исполняемых файлов для оценки их схожести, а также алгоритмов для автоматизации такого анализа.

Соискателем разработаны: метод формирования эталонных сигнатур программ и сигнатур идентифицируемых исполняемых файлов; метод сравнения сигнатур идентифицируемых исполняемых файлов с ранее сформированными эталонными сигнатурами программ; методика для идентификации исполняемых файлов на основе статического анализа характеристик дизассемблированного кода программ.

В диссертационной работе в качестве компонент модели представления исполняемого файла соискателем закономерно рассматриваются наиболее информативные, устойчивые в проявлении и независимые ассемблерные команды. Также рассматривается теория полезности, придающая различные коэффициенты относительной важности ассемблерным командам, что позволяет проявить их эмерджентное свойство.

– 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 качественному восприятию материала.

Отмеченные недостатки по содержанию автореферата не снижают качество исследований и не влияют на ценность теоретических и практических результатов диссертации.

Указанные в тексте автореферата работы отражают необходимую полноту опубликования результатов, а количество публикаций также свидетельствует о широкой их апробации на различных конференциях и семинарах, что, в том числе, отражает глубокую теоретическую и практическую проработку исследуемой темы и, соответственно, характеризует высокую степень обоснованности и достоверность полученных К.И. Салахутдиновой результатов, что также видно из текста автореферата.

Считаю, что представленная соискателем диссертационная работа – законченное самостоятельное исследование, обладающее актуальностью и новизной, отвечающее требованиям, изложенным в Положении о порядке присуждения ученых степеней.

Таким образом, К.И. Салахутдинова заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

инженер-программист 1ой категории
к.т.н. Спивак Антон Игоревич

«21» января 2020г. /Спивак А.И./

Сведения о составителе отзыва:
Фамилия, Имя, Отчество: Спивак Антон Игоревич
Ученая степень: к.т.н.
Место работы: ООО «АПСТЕК Лабс»
Должность: инженер-программист 1ой категории
Адрес:190020, Санкт-Петербург, наб. Обводного канала, д. 199-201, лит. «И», эт. 1, пом. 2.
Телефон: +78126475521
E-mail: anton.spivak@apstecsystems.com

Генеральный директор
ООО «АПСТЕК Лабс» Герасимов И.Н.

Подпись Спивака А.
удостоверяю.