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»

Важной научно-технической задачей в сфере информационной безопасности является повышение эффективности обеспечения и поддержания требуемого уровня защищенности обрабатываемой, хранимой и передаваемой информации. Это делает актуальными исследования в области изучения открытого программного обеспечения на персональных компьютерах и идентификации исполняемых файлов на основе уникальных характеристик.

Теоретическая значимость диссертации Салахутдиновой К.И. определяется научной новизной результатов, вынесенных на защиту, среди них:

1. Метод формирования эталонных сигнатур программ и сигнатур идентифицируемых исполняемых файлов, основанный на статическом подходе анализа характеристик дизассемблированных кодов программ; эффективность предложенных эталонов обеспечивается использованием для их построения уникальных по форме и амплитуде частотных распределений, отличающих специально образом отбираемые группы наиболее информативных ассемблерных команд, устойчиво проявляющихся в различных программах.

2. Метод сравнения сигнатур идентифицируемых исполняемых файлов с ранее сформированными эталонными на основе комбинированного использования градиентного бустинга деревьев решений как алгоритма машинного обучения и аддитивного критерия Фишберна; эта комбинация позволяет уменьшить число ошибок неверной классификации и максимизировать эмерджентность совокупности признакового пространства.

3. Методика идентификации исполняемых файлов, использующая разработанные метод формирования сигнатур идентифицируемых файлов и метод сравнения их с эталонными из архива; эта методика обеспечивает увеличение точности идентификации при комбинированном анализе характеристик исполняемых файлов, вычисляемых на основе их дизассемблированного представления.

Отраженные в автореферате результаты диссертации представлены на целом ряде всероссийских и международных конференций и опубликованы в изданиях,

индексируемых авторитетными наукометрическими базами. Это свидетельствует об их обоснованности и достоверности.

Практическая значимость вынесенных на защиту методов и методики заключается в том, что они могут быть использованы при построении систем автоматизированного аудита электронных носителей информации и предотвращения возникновения новых уязвимостей в автоматизированной системе.

Некоторые замечания по содержанию автореферата:

- 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.

Отмеченные недостатки не снижают общего положительного впечатления от приведенных в автореферате диссертации результатов. Работа Салахутдиновой К.И. представлена как завершенное и самостоятельное научное исследование, соответствующее требованиям «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства РФ от 24.09.2013 г. №842, предъявляемым 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».

Доктор физико-математических наук,
профессор кафедры информационных систем в экономике
Санкт-Петербургского государственного университета
ЮРКОВ А.В.

21 января 2020 года

Личную подпись

Сведения о составителе отзыва:

Фамилия, Имя, Отчество: Юрков Александр Васильевич
Ученая степень: доктор физико-математических наук
Ученое звание: старший научный сотрудник
Место работы: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет»
Должность: профессор кафедры информационных систем в экономике
Почтовый адрес: 191123, Санкт-Петербург, ул. Чайковского, 62
Телефон: +7 (812) 363-67-78
E-mail: a.v.yurkov@spbu.ru