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

Свободное программное обеспечение занимает обширную область среди современного программного обеспечения, пользователи которого, в частности, имеют права на его свободное использование и, что самое важное, модификацию. Большая часть открытого программного обеспечения разрабатывается под операционные системы Linux семейства Unix подобных систем.

Большое число современных исследований направлено на разработку методов детектирования или распознавания вредоносных программ, однако не только такое программное обеспечение может нести угрозы автоматизированной системе. Незаконное использование интеллектуальной собственности, нарушение авторских прав, использование некачественного программного обеспечения или приложений развлекательного характера, отвлекающих работника от его должностных обязанностей – всё это, не только способно нести угрозы конфиденциальности, доступности и целостности обрабатываемой на компьютерах информации, но также стать потенциальным источником уязвимостей.

Все вышеописанное ведет к тому, что аудит электронных носителей информации на предмет выявления несанкционированно установленного программного обеспечения становится важной и всё более актуальной задачей. Разработанная методика позволяет выявить нарушения установленной политики безопасности при обработке конфиденциальной информации.

Научная новизна проведённого исследования и личный вклад автора:

1. Метод формирования профиля исполняемого файла, позволяет представить состояние программы в виде уникальной информативной последовательности, делающей возможным проводить на её основе сравнение различных программ.
2. Использование возможностей комбинированного использования машинного обучения и теории полезности для формирования метода сравнения сигнатур.
3. Итерационный процесс сравнения независимых профилей исполняемых файлов в совокупности с постобработкой результатов кластеризации составляют методику идентификации исполняемых файлов, предоставляющую возможность производить распознавание программы, не основываясь на целостности её данных.

Основные положения опубликованы в ведущих научных журналах, доложены на представительных научных конференциях и подтверждены экспериментально. Федеральной службой по интеллектуальной собственности зарегистрировано 5 программ для ЭВМ (в соавторстве) и 1 программа для ЭВМ (личного авторства). Имеется 3 акта о внедрении результатов работы.

Все это свидетельствует об объективности, достоверности и практической ценности полученных результатов.

В качестве замечаний к автореферату можно отметить следующее:

1. В описании четвёртой главы отсутствует информация о характеристиках рассматриваемых исполняемых файлах, что не дает возможность получить представление о проведенных экспериментальных исследованиях.

2. В работе рассматриваются исполняемые файлы формата ELF, однако не говорится о том, возможно ли применение разработанной методики к исполняемым файлам других форматов, например, PE.

После ознакомления с авторефератом можно сделать вывод, что, невзирая на приведённые замечания, диссертационная работа Салахутдиновой Ксении Иркиновны является законченным научно-исследовательским трудом, выполненным автором самостоятельно на высоком техническом уровне. Полученные результаты обладают практической значимостью и достаточной степенью научной новизны, решая актуальную научно-техническую задачу по повышению эффективности мониторинга персональных компьютеров автоматизированной системы и идентификации установленного на них программного обеспечения.

Работа Салахутдиновой К.И. отвечает всем требованиям «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства РФ от 24.09.2013 г. № 842, а её автор заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Заведующий кафедрой Информатики
и информационной безопасности
Северного (Арктического)
федерального университета,
канд. техн. наук, доцент
«_20_» _января_ 2020 г. И.И. Василишин

Личную подпись Василишина И.И.
заверяю: ученый секретарь ученого совета САФУ
Е.Б. Раменская
«20» января 2020 г.

Сведения о составителе отзыва:
Фамилия, Имя, Отчество: Василишин Игорь Иванович
Ученая степень: канд. техн. наук
Ученое звание: доцент
Место работы: Северный (Арктический) федеральный университет
Должность: Заведующий кафедрой Информатики и информационной безопасности
Почтовый адрес: 163007, г. Архангельск, наб. Северной Двины, 2, каб. 10-301.
Телефон: +7-911-568-61-51
E-mail: i.vasilishin@agtu.ru