ОТЗЫВ

на автореферат диссертации Салахутдиновой Ксении Иркиновны «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

Как следует из автореферата, диссертация Салахутдиновой К.И. посвящена открытому программному обеспечению формата ELF, повсеместно распространенному и широко используемому. Такое программное обеспечение свободно распространяется и поддерживается разработчиками в актуальном состоянии, за счет выпуска новых версий, порой отличающихся от предыдущих незначительно.

Рост популярности и активного использования открытого программного обеспечения, и, соответственно, возрастающая необходимость обеспечения достаточного уровня безопасности информации, циркулирующей в локальной сети предприятия говорят об актуальности диссертационной работы. В связи с тем, что на средствах вычислительной техники, используемых пользователями, происходят информационные процессы, на которые может происходить нежелательное влияние со стороны непроверенного программного обеспечения. При этом существующие методы защиты информации не в достаточной мере подходят для проведения качественного мониторинга электронных носителей информации (как встроенных, так и съемных). Соискатель предлагает новые методы и методику по идентификации исполняемых файлов формата ELF.

Успешное решение задачи повышения эффективности идентификации исполняемых файлов достигается соискателем благодаря выбору нового оптимального набора характеристик программ, использованию наиболее подходящего алгоритма машинного обучения и применению теории полезности. Результаты работы подтверждаются большим количеством экспериментов.

Практическая значимость работы состоит в возможности использования результатов диссертационной работы при построении систем мониторинга средств вычислительной техники и формированию дополнительных мер по нейтрализации возникающих уязвимостей по причине эксплуатации некачественных или специальных программ.

Кроме того, результаты диссертационной работы внедрены в различных проектах, коммерческих и образовательных организациях, апробированы на множестве конференций, опубликованы в журналах ВАК, Scopus и других печатных

изданиях. Более того, соискателем получены свидетельства о регистрации компьютерных программ.

В процессе ознакомления с авторефератом были сформулированы следующие замечания:

1) В автореферате перечислены компьютерные программы, разработанные в процессе исследования, однако не упоминается возможность создания комплексного программного продукта, представляющего собой самостоятельный блок автоматического мониторинга средств вычислительной техники.

2) На странице 3 автореферата, говорится: «Возможные дефекты программного обеспечения … могут привести к росту числа уязвимостей и повлиять на информационную безопасность систем» однако отсутствует описание возможных уязвимостей и способов их эксплуатации.

Указанные недостатки не являются критическими и не снижают научной и практической ценности диссертационной работы, учитывая глубину проведенного исследования.

Таким образом, диссертация соответствует всем требованиям пп. 9 - 14 «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».

Зам. директора по науке СПбФ ИЗ]

д.т.н., профессор А. Г. Коробейников

25 декабря 2019 г.

Организация: Санкт-Петербургский филиал Федерального государственного бюджетного учреждения науки Института земного магнетизма, ионосферы и распространения радиоволн им. Н.В.Пушкова Российской академии наук. (СПбФ ИЗМИРАН)

http://izmiran.nw.ru

Адрес организации: 199034, Россия, Санкт-Петербург, Университетская наб, д.5, лит. Б.

Рабочий телефон: +7 (812) 323-28-07

Адрес эл. почты: Korobeynikov_A_G@mail/ru

ФИО рецензента: Коробейников Анатолий Григорьевич, д.т.н., профессор

Должность: заместитель директора по науке