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»

Контроль установленных программ представляет собой важную составляющую в организации защищенного функционирования бизнес-процессов. Возросшая популярность и повсеместное применение компьютерных технологий способствует не только прогрессу в области автоматизации процессов и обеспечения информационной безопасности автоматизированных систем, но и увеличению интереса к ним со стороны злоумышленников. Средства вычислительной техники позволяют использовать различное программное обеспечение для осуществления процессов анализа, управления, принятия решений. На существующие способы и методы защиты информации устанавливаются ограничения, связанные с особенностями процессов деятельности и аппаратно-техническим комплексом: разнообразие программ, возможное наличие портативного (не устанавливаемого) программного обеспечения, ограниченность числа версий конкретной программы, приводят к возрастающей сложности формирования уникальных шаблонов исполняемых файлов, и следовательно, вероятность пропуска несанкционированно установленного программного обеспечения возрастает. В соответствии с вышесказанным, работа Салахутдиновой К.И. Обладает актуальностью, так как направлена на распознавание программ и учитывает поставленные ограничения.

Формализованная постановка научной задачи свидетельствует о научной грамотности соискателя и позволяет лучше понять содержание работы. В диссертации поставлена и успешно решена задача повышения точности идентификации исполняемых файлов на электронных носителях информации. Положительные результаты получены благодаря использованию новой комбинации идентификационных признаков, формирующих модель представления исполняемого файла, применению новых методов формирования и сравнения сигнатур программ, на основе статического анализа дизассемблированного кода программ и комбинированного использования машинного обучения и теории полезности, а также использованию методики идентификации, соединяющей в себе теоретические положения и практические результаты в виде элементов комплексного подхода проведения аудита.

Работа Салахутдиновой К.И. Является практически значимой, поскольку представляется возможным использование не только теоретических результатов в качестве базы для дальнейших исследований, но и применение практических результатов в комплексе систем обнаружения преодоления запрета на установку программ и систем мониторинга состояния локальной сети, а также для проектирования и внедрения в защищенные автоматизированные системы обработки конфиденциальной информации. Более того, результаты работы могут быть интересны не только в задачах обеспечения информационной безопасности, но и в более общих задачах по классификации объектов.

Достоверность полученных результатов обеспечивается корректным использованием методического аппарата, положений математической статистики, теории информации и теории вероятности.

Как следует из автореферата, диссертантом успешно решены все поставленные в диссертационном исследовании задачи. Разработанные новые методы и методика могут применяться для различных задач идентификации исполняемых файлов. Результаты диссертационного исследования прошли достаточную апробацию и обсуждение на научных и научно-практических конференциях.

В качестве замечаний по автореферату необходимо отметить наличие некоторых стилистических погрешностей в тексте, а также описание предложенной методики идентификации исполняемых файлов представлено автором слишком кратко.

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

Результаты исследований автора, судя по автореферату, отвечают в полной мере требованиям, предъявляемым к кандидатским диссертациям по специальности 05.13.19 «Методы и

системы защиты информации, информационная безопасность». Автореферат диссертации составлен с соблюдением установленных требований, дает полное представление о содержании работы. Основные положения выполненных исследований нашли отражение в 8 публикациях автора, в изданиях, рекомендованных ВАК, в 8 публикациях, индексируемых Scopus и внедрены в различных научно-исследовательских проектах. Качество разработанных программных продуктов подтверждается наличием свидетельств регистрации программ для ЭВМ государственного образца.

На основании содержания автореферата, можно полагать, что представленная работа отвечает всем требованиям ВАК, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность, а ее автор Салахутдинова Ксения Иркиновна заслуживает присуждения ей ученой степени кандидата технических наук.

Руководитель проектов
кандидат технических наук
Лапшин Сергей Владимирович
«23» января 2020 г

Сведения о составителе отзыва
Лапшин Сергей Владимирович
Кандидат технических наук
Руководитель проектов
ООО «Цезурити»

Подпись верна
Генеральный директор

197343
Россия, Санкт-Петербург,
ул. Матроса Железняка, 57

+7 (812) 640 41 43
antivirus@cezurity.com