АКЦИОНЕРНОЕ ОБЩЕСТВО
«НПК «ТРИСТАН»
ул. 2-я Боевская, д. 2, Москва, 107014
тел.: (495)603-09-31, факс: (495)603-09-29
e-mail: 3stan@3stan.ru
САНКТ-ПЕТЕРБУРГСКИЙ ФИЛИАЛ
пр. Непокорённых, д.47, г. Санкт-Петербург, 195220
тел.: (812)535-22-46, факс: (812)535-27-16
e-mail: spb-tristan@mail.ru
ОКПО 60966329 ОГРН 1037739256158
ИНН 7718213897 КПП 780443001

УТВЕРЖДАЮ

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА

И.Н. Соловьев

«20» января 2020 г.

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»

Текущее состояние развития информационных технологий позволяет расширить возможности по осуществлению процессов анализа, управления, принятия решений. Большинство операций теперь производится на компьютерах, способных одновременно решать множество разноплановых задач. Становится очевидным необходимость в реализации наиболее полной и комплексной защиты автоматизированных систем и обрабатываемой на них информации.

Диссертационная работа Салахутдиновой К.И. связана с обеспечением информационной безопасности автоматизированных систем, а именно с идентификацией исполняемых файлов на электронных носителях информации. Тематика работы является **актуальной**, поскольку автоматизированные системы стали неотъемлемой частью коммерческих и государственных организаций, однако уровень информационной безопасности в компьютерных сетях и системах недостаточен, а существующие методы идентификации исполняемых файлов имеют ряд ограничений.

В работе учтены такие особенности исполняемых файлов, как:

- потенциальное количество различных программ, установленных на одном компьютере или на всех компьютерах организации;
- количество различных версий для каждой программы, измеряемое от одной до десятков, но в практике не превосходящее сотни;
- наличие существенных изменений в различных версиях одной программы;
- наличие индивидуального характера распределения признака идентифицируемого файла от других программ.

Благодаря предложенным модели представления исполняемого файла, методам формирования и сравнения сигнатур программ, методике идентификации исполняемых файлов Салахутдинова К.И. **успешно решила задачу** увеличения точности идентификации исполняемых файлов на электронных носителях информации. Результаты работы подтверждены многочисленными экспериментами.

Теоретическая значимость работы состоит в возможности дальнейшего развития научно-методического аппарата по идентификации исполняемых файлов и решении

исследуемой области, а также повышении гибкости существующих систем обнаружения несанкционированно установленного программного обеспечения.

Практическая значимость работы состоит в возможности использования результатов диссертационной работы при организации процесса аудита информационной безопасности автоматизированных систем. Также результаты полученные Салахутдиновой К.И. могут служить основой для тестирования на уникальность программного обеспечения среди конкурентных продуктов схожей функциональности.

Апробация представленного научно-методического аппарата, а именно модели представления исполняемого файла, метода формирования сигнатур программ, метода сравнения сигнатур и методики идентификации осуществлена на различных конференциях. Результаты работы реализованы в нескольких НИР, опубликованы в печатных изданиях, в том числе 8 публикаций в журналах ВАК, получено 6 свидетельств о регистрации программного обеспечения.

К автореферату диссертации были сформулированы следующие **замечания:**

1. Остается не до конца ясным на основе какого принципа происходит выбор конкретных ассемблерных команд и какое число ассемблерных команд участвует в анализе их информативности.
2. В тексте автореферата упоминается тестирование различных алгоритмов машинного обучения и статистических критериев, однако не вполне ясно, учитывается ли вычислительная сложность алгоритмов при их оценке эффективности.

Приведенные замечания не снижают в целом **положительной оценки** диссертационной работы, выполненной в соответствии с пунктами 9-14 Положения о присуждении ученых степеней, утвержденного постановлением РФ от 24 сентября 2013г. №842.

Соискатель Салахутдинова К.И. **заслуживает** присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Отзыв составил
Заместитель директора по программному обеспечению,
Санкт-Петербургский филиал АО «НПК «ТРИСТАН»,
кандидат технических наук

Шахпаронян Артём Павлович