ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА» (СПбГУТ)

ОТЗЫВ

на автореферат диссертации Салахутдиновой Ксении Иркиновны «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»

Возрастающая тенденция к применение открытого, свободно распространяемого программного обеспечения с одной стороны становится неотъемлемой частью деятельности современных информационных систем, эксплуатируемых в различных секторах экономики, позволяющей расширить возможности по осуществлению различных процессов, с другой стороны – обуславливает необходимость дополнительных мер и методов защиты информации. Не санкционированно установленное программное обеспечение может не только стать лазейкой для противоправных действий нарушителя информационной безопасности, путем подмены или модификации исполняемых файлов, но также привести к критическим ошибкам системы, способным остановить отлаженные бизнес-процессы, замедлить работу автоматизированной системы, повлиять на работоспособность персонала.

Таким образом, тема исследования диссертационной работы Салахутдиновой К.И., посвященная решению задач по разработке методов и алгоритмов автоматизированной идентификации исполняемых файлов, является своевременной и актуальной.

Существующие подходы к идентификации установленного программного обеспечения обладают рядом ограничений и недостаточными возможностями по обеспечению комплексной реализации мер информационной безопасности и реализованы, в основном, не для свободно распространяемого программного обеспечения, в котором динамика появления новых версий и обновлений существенно ниже, чем для открытого программного обеспечения. Предлагаемые в автореферате диссертации методы и методика их применения, учитывают и эту особенность.

Поэтому, научная новизна и теоретическая значимость основных результатов проведенного соискателем диссертационного исследования не вызывают сомнения и состоит в:

- разработанном методе формирования сигнатур идентифицируемых исполняемых файлов и эталонных сигнатур программ, основанном на

анализе структурных характеристик дизассемблированного представления программного обеспечения. Метод включает в себя ряд отобранных наиболее информативных и устойчивых в проявлении ассемблерных команд, на основе которого производится реализация алгоритма формирования частотных распределений – сигнатур;

- разработанном методе сравнения сигнатур идентифицируемых исполняемых файлов с ранее сформированными эталонными сигнатурами программ, основанном на сочетании метода машинного обучения и аддитивного критерия, позволяющего достигать увеличение точности идентификации за счет совокупного использования признакового пространства;
- разработанной методике идентификации исполняемых файлов, основанной на итерационном процессе применения разработанных методов, способной производить мульти-классификацию версий программ, ранее не задействованных в создании эталонных сигнатур исполняемых файлов, в условиях большого числа различных наименований программ и ограниченности числа объектов обучающей выборки.

Практическая значимость результатов исследования, отмеченных в тексте автореферата, заключается в повышении функциональной эффективности аудиторской деятельности по обеспечению заинтересованных организаций актуальной и достоверной информацией об используемом программном обеспечении. Этот факт подтверждается проведенными экспериментальными расчетами с использованием программной реализации и полученными актами о внедрении результатов исследования.

По теме диссертационного исследования опубликовано 32 работы, среди которых 8 – в журналах, рекомендованных для опубликования научных результатов соискателей ВАК РФ, 8 – в журналах, индексируемых в системах цитирования Scopus и Web of Science, и 10 – в трудах конференций. Также зарегистрировано 6 программ для ЭВМ.

Автореферат Салахутдиновой К.И. написан корректно, научным языком и в достаточной степени отражает суть проведенных исследований. Из основных положений, представленных в автореферате соискателя, можно сделать вывод о соответствии диссертации паспорту специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Тем не менее, при общей положительной оценке содержания автореферата следует отметить следующие замечания:

- в автореферате приводятся результаты трех способов оценки точности идентификации: матрицы ошибок (Confusion Matrix), точности (Accuracy), бикубической меры (F-measure), однако из текста автореферата не ясна причина выбора такого числа и именно таких способов оценки;
- в автореферате приводятся результаты проведенных экспериментов с целью проверки достигаемой точности идентификации при помощи разработанной методики, однако отсутствует описание рассматриваемой выборки: ее

объем, функциональная направленность программ, число различных версий, способ дизассемблирования и т.п.

Указанные замечания по автореферату не снижают общую положительную оценку научного уровня проведенного диссертационного исследования.

Заключение. Диссертационная работа Салахутдиновой К.И. является научно-квалификационной работой, в которой отражено решение важной и актуальной научно-технической задачи – разработки методики идентификации исполняемых файлов на основе статического анализа характеристик дизассемблированного кода программ. Диссертация соискателя удовлетворяет требованиям пп. 9-14 «Положения о присуждении ученых степеней», предъявляемым к кандидатским диссертациям, а ее автор, Салахутдинова Ксения Иркиновна, заслуживает присуждения ей ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Доцент кафедры Безопасности информационных систем СПбГУТ,
кандидат физико-математических наук, доцент

«24» января 2020 г. __ ___ / А.Н. Кривцов /

Сведения о составителе отзыва:

Фамилия, Имя, Отчество: Кривцов Александр Николаевич
Ученая степень: кандидат физико-математических наук
(специальности 05.13.11 и 01.01.09)
Ученое звание: доцент
Место работы: Санкт-Петербургский Государственный университет
Телекоммуникаций им. проф. М.А. Бонч-Бруевича
Должность: доцент кафедры Безопасности информационных систем
Почтовый адрес: 193232, г. Санкт-Петербург, пр. Большевиков, д.22,
Телефон: (812) 326-08-89
E-mail: a_kriv@mail.ru

А.Н. Кривцова
Отдела кадров - зам. начал
/В.В. Новикова/ 24