ОТЗЫВ

научного руководителя о кандидатской диссертации М.А. Казачук «Динамическая аутентификация пользователей на основе анализа работы с клавиатурой компьютера», представленной на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

М.А. Казачук (1993 г.р.) поступила на первый курс факультета Вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова в 2010 г. и окончила его с отличием в 2015 г. С 2015 по 2019 гг. М.А. Казачук проходила обучение в очной аспирантуре факультета и окончила ее с отличием. В настоящее время работает в должности математика в лаборатории Технологий программирования кафедры Интеллектуальных информационных технологий. М.А. Казачук принимает активное участие в работе спецсеминара «Вопросы распределенной обработки информации», руководит курсовыми и дипломными работами студентов, является соавтором и лектором обязательного курса магистратуры кафедры ИИТ факультета ВМК МГУ «Современные методы распределенного хранения и обработки данных», а также ведет семинарские занятия по практикуму на ЭВМ на втором курсе ВМК МГУ.

Перед диссертантом была поставлена задача исследовать возможность применения методов машинного обучения и интеллектуального анализа данных для решения задачи динамической аутентификации пользователей на основе анализа их клавиатурного почерка. Решение задач такого типа является важной составляющей обеспечения компьютерной безопасности во всем мире. Основная сложность задачи состоит в том, что работа ведется над данными высокой размерности, содержащими множественные корреляции. Существующие в данной области решения имеют ряд существенных недостатков. В частности, они показывают недостаточно высокое качество работы (точность порядка 85–90%, ROC AUC ниже 0.90), не способны выделять стабильные по времени признаковые характеристики и не предлагают способ агрегационной оценки степени аномальности поведения пользователя за продолжительный период его работы за компьютером.

Для решения обозначенных выше алгоритмических проблем, М.А. Казачук были предложены:

- Подход к подготовке данных, описывающих клавиатурный почерк пользователя, включающий в себя способ построения признакового пространства и подход к дальнейшей обработке признаков на основе

дискретизации их по квантилям. Сокращение размерности признакового пространства производится путем отбора наиболее значимых признаков с использованием критерия Колмогорова-Смирнова. Экспериментально установлено, что данный подход позволяет построить пространство стабильных по времени признаковых характеристик;

- Нечеткий метод выявления аномалий в данных на основе эллиптической кластеризации (ESFC) в RKHS, строящий в пространстве высокой размерности эллиптические области с оптимальным центром для выявления аномалий. Подбор оптимальных значений метапараметров данного алгоритма осуществляется собственно разработанным методом, строящим стабильные к смене тестового набора данных одноклассовые модели без использования информации о данных нелегитимного класса. Оценка аномальности поведения пользователя производится как за короткий, так и за продолжительный период работы – с использованием разработанного метода оценки аномальности поведения пользователей на основе анализа целых сессий работы за компьютером с использованием t-статистики Уэлша. По результатам экспериментов, метод ESFC превзошел качество распознавания существующих алгоритмов при классификации как отдельных векторов признаков, так и целых сессий работы пользователей за компьютером.

Автором разработан и реализован экспериментальный образец программного комплекса (ЭО ПК), использующий комбинацию предложенных алгоритмов для осуществления динамической аутентификации пользователей по клавиатурному почерку, показывающий высокое качество работы (превышающее качество аутентификации существующих решений) и обладающий высокой производительностью, а также свойствами масштабируемости (возможностью распределять программные компоненты по разным физическим машинам) и расширяемости (возможностью добавлять либо заменять отдельные программные модули и компоненты).

М.А. Казачук провела всестороннее исследование рассматриваемой в работе проблемы и проявила себя самостоятельным, целеустремленным и трудолюбивым исследователем. В ходе работы над диссертацией Казачук М.А. показала владение современными методами машинного обучения, интеллектуального анализа данных, математической статистики, а также методами линейной алгебры, математического анализа, объектно-ориентированного анализа и проектирования, проявила умение формулировать гипотезы, осуществлять их экспериментальную проверку, выполнять программную реализацию предложенных алгоритмов.

Полученные автором результаты являются новыми, аналитически обоснованными, подтвержденными большим объемом экспериментальных исследований и нашли применение в НИР «Разработка технологий биометрической идентификации пользователя по признакам, проявляющимся при использовании устройств ввода данных персональных ЭВМ» (Номер договора №01-04/15 от 08 апреля 2015 г), 2015–2017 гг. Результаты работы были опубликованы автором в виде семи научных публикаций (три из которых опубликованы в изданиях, рецензируемых Web Of Science, Scopus и RSSI), а также представлены на шести всероссийских и международных научных конференциях. Разработанные алгоритмы перспективны как с математической, так и с прикладной точки зрения, и могут применяться в перспективных интеллектуальных системах информационной безопасности, основанных на анализе компьютерной поведенческой информации, на этапах построения и обработки признакового пространства, а также построения и применения модели пользователя.

Представленная работа удовлетворяет всем требованиям, предъявляемым к кандидатским диссертациям, выполнена на высоком научном уровне, представляет собой законченное научное исследование. Ее результаты получены лично автором и прошли квалифицированную апробацию. Автореферат правильно отражает содержание диссертации. Рекомендую присудить ее автору М.А. Казачук ученую степень кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Научный руководитель
Петровский Михаил Игоревич,
кандидат физико-математических наук,
доцент факультета Вычислительной математики и кибернетики
МГУ имени М.В. Ломоносова,
кафедра Интеллектуальных информационных технологий
(119991, Москва, Ленинские горы, д.1, стр. 52)
Рабочий телефон: +7 (495) 939-17-89
Адрес электронной почты: michael@cs.msu.su
16.09.2019

Подпись М.И. Петровского заверяю.

Российская Федерация * Московский государственный университет имени М.В. Ломоносова * Факультет вычислительной математики и кибернетики * г. Москва
ОТДЕЛ КАДРОВ

Подпись удостоверяю
Ведущий специалист по кадрам
Т.Г. Коваленко
23.09.2019г.