ОТЗЫВ

научного руководителя о диссертационной работе

Браницкого Александра Александровича

«Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Браницкий А.А., 1990 года рождения, в 2012 году с отличием окончил математико-механический факультет Санкт-Петербургского государственного университета по специальности «Математическое обеспечение и администрирование информационных систем». С 2015 года по настоящее время работает в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН) в должности младшего научного сотрудника. В 2016 году с отличием окончил очную аспирантуру СПИИРАН по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Диссертационная работа Браницкого А.А. посвящена разработке модельно-методического аппарата для обнаружения аномальных соединений в сетевом трафике. Основные результаты, полученные диссертантом, следующие:

1. модель искусственной иммунной системы на базе эволюционного подхода для классификации сетевых соединений;
2. алгоритм генетико-конкурентного обучения сети Кохонена для обнаружения аномальных сетевых соединений;
3. методика иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений;
4. архитектура и программная реализация распределенной системы обнаружения атак, построенной на основе гибридизации методов вычислительного интеллекта и сигнатурного анализа.

Полученные результаты были представлены на нескольких российских и международных конференциях: “Информационные технологии в управлении” (2012 г., 2016 г.), “Информационная безопасность регионов России” (2015 г., 2017 г.), “Региональная информатика” (2016 г.), восемнадцатой IEEE международной конференции по вычислительным наукам и инжинирингу (2015 г.), международной

конференции по математическим методам, моделям и архитектурам систем защиты компьютерных сетей (2017 г.) и др.

В процессе написания кандидатской диссертации Браницкий А.А. принимал активное участие в нескольких научно-исследовательских проектах, а именно в гранте РНФ "Управление инцидентами и противодействие целевым кибер-физическим атакам в распределенных крупномасштабных критически важных системах с учетом облачных сервисов и сетей Интернета вещей", проекте Минобрнауки России "Разработка технологий интерактивной визуализации неформализованных данных разнородной структуры для использования в системах поддержки принятия решений при мониторинге и управлении информационной безопасностью информационно-телекоммуникационных систем", проекте Минобрнауки России "Перспективные методы корреляции информации безопасности и управления инцидентами в критически важных инфраструктурах на основе конвергенции технологий обеспечения безопасности на физическом и логическом уровнях".

Во время выполнения научно-исследовательской деятельности Браницкий А.А. зарекомендовал себя как грамотный научный сотрудник, способный корректно ставить и решать научно-технические задачи, проявил самостоятельность, целеустремленность и трудолюбие при подготовке научных статей и проведении экспериментальных исследований. Выбранная диссертантом тема исследований является актуальной, а полученные им результаты соответствуют современному состоянию решаемой проблемы. Об этом свидетельствует наличие опубликованных с его авторством 6 работ, рекомендованных ВАК, и 3 работ, индексируемых в системах Web of Science и Scopus.

Браницкий А.А. является специалистом в области сетевой безопасности, системного программирования и искусственного интеллекта, что позволило ему успешно выполнить все поставленные в диссертационной работе задачи. Отмечаю его творческий подход к постановке и решению задач, инициативность и ответственность, которые характеризуют его как состоявшегося ученого в области информационной безопасности.

Полученные диссертантом теоретические результаты являются важными при решении таких задач, как разработка систем обнаружения атак, классификация многомерных объектов при помощи комбинированных подходов, обнаружение аномальных соединений в сетевом трафике.

Кандидатская диссертация Браницкого А.А. является завершенной научно-квалификационной работой, выполненной на высоком теоретическом уровне и содержащей научно обоснованные результаты в области обнаружения аномальных сетевых соединений. Данные результаты имеют весомое практическое значение, что подтверждают 3 свидетельства о регистрации программ для ЭВМ и 3 акта о внедрении результатов в учебных заведениях. Считаю, что диссертационная работа Браницкого Александра Александровича полностью отвечает всем требованиям п. 9 «Положения ВАК Минобрнауки РФ», предъявляемым ВАК Министерства науки и образования России к кандидатским диссертациям, и может быть представлена к защите на диссертационном совете Д.002.199.01 при Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук по научной специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Научный руководитель
Доктор технических наук, профессор,
главный научный сотрудник лаборатории проблем компьютерной безопасности
Федерального государственного бюджетного учреждения науки Санкт-Петербургского
института информатики и автоматизации Российской академии наук (СПИИРАН)

Котенко Игорь Витальевич

14 июня 2018 г.
Рабочий адрес: 199178, Санкт-Петербург, ВО 14 линия, дом 39
Тел. +7-(812)-328-71-81
E-mail: ivkote@comsec.spb.ru