ОТЗЫВ

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

В диссертационной работе Браницкого А.А. решается важная научно-техническая задача – разработка модельно-методического аппарата для обнаружения аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта. Актуальность выбранного направления обусловлена разнообразием и ростом числа сетевых атак в компьютерных сетях, что требует разработки алгоритмов, методик и программных инструментов, предназначенных для обнаружения сетевых атак.

Представленный в диссертационной работе подход, совмещающий сигнатурный анализ и методы вычислительного интеллекта, позволяет повысить эффективность функционирования системы обнаружения атак за счет построения разнообразных схем объединения бинарных классификаторов. Для выполнения этой цели были разработаны оригинальные модель искусственной иммунной системы на безе эволюционного подхода, алгоритм генетико-конкурентного обучения сети Кохонена, методика иерархической гибридизации бинарных классификаторов, а также архитектура программного прототипа системы обнаружения атак. С помощью разработанного программно-аппаратного стенда выполнены эксперименты по генерации набора данных и оценке эффективности предложенных автором модели, алгоритма, методики и архитектуры.

В автореферате были обнаружены следующие недостатки:

1. Не обоснован выбор требований, предъявляемых к вычислительно интеллектуальным системам и в частности к разработанной системе обнаружения атак.
2. Не обоснован выбор ОС Linux в качестве платформы для проведения экспериментов.

Судя по автореферату, данная диссертационная работа представляет собой законченное самостоятельное исследование и, несмотря на наличие вышеупомянутых недостатков, выполнена на высоком теоретическом уровне в

соответствии с требованиями п. 9 «Положения о порядке присуждения ученых степеней», предъявляемыми ВАК к кандидатским диссертациям. Считаю, что Браницкий А.А. заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Доцент кафедры сетей связи и передачи данных СПбГУТ
к.т.н.
«12» сентября 2018г.

Сведения о составителе отзыва:
ФИО: Пантюхин Олег Игоревич
ученая степень: кандидат техни
ученое звание: доцент
место работы: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича
должность: доцент кафедры сетей связи и передачи данных
почтовый адрес: пр. Большевиков д. 22, корп. 1, Санкт-Петербург, 193232
тел.: (812)305-12-84
электронная почта: p_oleg99@mail.ru