Общество с ограниченной ответственностью «Инновационный центр транспортных исследований»
199155, Санкт-Петербург, пр. КИМа, д.4,
литер Б, помещение 25-Н
тел./факс (812) 350-38-26,
E-mail: innotech@bos.ru
ОГРН 1117847711387
ИНН 7801564509, КПП 780101001

06.09.2018 № 17/2018

В диссертационный совет Д 002.199.01
при Федеральном государственном
бюджетном учреждении науки Санкт-
Петербургском институте информатики и
автоматизации Российской академии наук

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».

Актуальность темы диссертации

Диссертационная работа Браницкого А.А. посвящена решению важной научной задачи – разработки модельно-методического аппарата для обнаружения аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта. Предложенный подход позволяет повысить эффективность функционирования сетевых систем обнаружения атак (СОА). Востребованность в разработке подобных систем вызвана необходимостью обеспечения информационной безопасности критически важных объектов в различных отраслях человеческой деятельности и постоянным интересом научно-исследовательского общества к развитию модельно-алгоритмического аппарата в области информационной безопасности и, в частности, в области обнаружения сетевых атак. Это подтверждает актуальность выбранной Браницким А.А. темы исследований.

Научная новизна

В рамках диссертационного исследования получены четыре научных результата. В первом результате предложена новая модель иммунной системы,

которая позволяет снизить уровень ложных срабатываний в СОА за счет двухступенчатого алгоритма обучения иммунных детекторов. Второй результат включает алгоритм обучения сети Кохонена, для повышения сходимости которого предложено несколько стратегий генетической оптимизации весов искусственных нейронов; предложенная оптимизация позволяет сократить время настройки СОА. Третий результат – методика иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений; разработанная методика позволяет объединить разнородные механизмы обнаружения сетевых атак, в том числе разнообразные методы вычислительного интеллекта и сигнатурный анализ, и отличается от известных наличием «ленивого» подключения узловых классификаторов, что позволяет сократить время на анализ сетевого трафика. В четвертом результате представлена архитектура разработанного прототипа сетевой СОА; новизна этого результата заключается в совместном использовании разработанных модели, алгоритма и методики.

Достоверность научных положений

Достоверность изложенных четырех положений подтверждается успешной апробацией на нескольких научных конференциях, а также согласованностью теоретических результатов с результатами, полученными в ходе проведения экспериментов. По результатам диссертационного исследования опубликовано шесть статей в журналах, рекомендованных ВАК Министерства науки и образования России и три статьи – в зарубежных изданиях, индексированных в Web of Science и Scopus.

Практическая значимость

Полученные результаты могут быть применены при построении компонентов СОА, а также в качестве основы для решения задач классификации объектов. Практическая значимость предложенного подхода заключается в повышении эффективности функционирования СОА и подтверждается наличием нескольких актов внедрения и свидетельств о регистрации программ для ЭВМ.

Замечания по автореферату

Следующие замечания имеют место быть:

1. На странице 12 говорится об извлечении 106 параметров, характеризующих сетевые соединения, однако не указана размерность сжатого вектора признаков, полученного в результате применения метода главных компонент.
2. Из текста автореферата непонятно, каким образом получен набор данных, содержащий три класса сетевых соединений (стр. 14), и что он из себя представляет.

Заключение

Указанные замечания не снижают научной ценности полученных результатов. Данная диссертационная работа является завершенным научным исследованием, обладает актуальностью и новизной. Считаю, что выполненная Браницким А.А. диссертационная работа удовлетворяет требованиям п. 9 «Положения ВАК Минобрнауки РФ», предъявляемым ВАК Министерства науки и образования России к кандидатским диссертациям, а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Отзыв подготовил:
И.О. генеральн
ООО «Иннова исследований»
д.т.н., с.н.с. Чернов В.Ю.
06 сентября 20

Сведения о со
ФИО, ученая димир Юрьевич, доктор технических наук, стар
Место работы: ООО «Инновационный центр транспортных исследований»
Должность: И.О. генерального директора
Тел.: (812)3503826
Почтовый адрес: г. Санкт-Петербург, пр. КИМа, д. 4, пом. 25-Н, 199155
Электронная почта: innotech@bos.ru