АКЦИОНЕРНОЕ ОБЩЕСТВО «КОНЦЕРН РАДИОСТРОЕНИЯ «ВЕГА»
ФИЛИАЛ В Г. САНКТ- ПЕТЕРБУРГЕ
JOINT- STOCK COMPANY «RADIO ENGINEERING CORPORATION «VEGA»
BRANCH IN ST. PETERSBURG

_____ № 87/_____

На №_____ от_____

Ученому секретарю
диссертационного совета
Д 002.199.01
А.А. Зайцевой

14 линия, д.30,
г. Санкт-Петебург, Санкт-
Петербургский институт
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»

Успешно реализованные сетевые атаки оказывают негативное воздействие на функционирование сетевых ресурсов. В частности такие действия могут приводить к частичной приостановке обслуживания клиентских запросов или вовсе к отказу и полному выходу из строя сетевого оборудования. Поэтому решаемая в диссертационном исследовании задача обнаружения сетевых атак и сетевых аномалий в компьютерных сетях является актуальной.

ул. Академика Павлова, д. 14-а, г. Санкт-Петербург, Россия, 197376
Телефон: (812) 438-76-54
Факс: (812) 438-76-54
E-mail: mail@spb.vega.su

ul. AcademicaPavlova, d.14-a, St. Petersburg, Russia, 197376
Phone: (812) 438-76-54
Fax: (812) 438-76-54
E-mail: mail@spb.vega.su

Основная цель, поставленная в диссертационной работе, заключается в повышении эффективности функционирования системы обнаружения атак (СОА). Автор выносит на защиту ряд положений, а именно (1) модели искусственной иммунной системы на базе эволюционного подхода для классификации сетевых соединений, (2) алгоритма генетико-конкурентного обучения сети Кохонена для обнаружения аномальных сетевых соединений, (3) методики иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений, (4) архитектуры и программной реализации распределенной СОА, построенной на основе гибридизации методов вычислительного интеллекта и сигнатурного анализа.

Научная новизна предложенного подхода заключается в построении модели искусственной иммунной системы на базе эволюционного подхода для классификации сетевых соединений с использованием механизмов постоянного обновления иммунных детекторов с учетом текущего этапа их зрелости, гибким заданием вложенности классификаторов друг в друга в предлагаемой методике иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений.

Практическая значимость предложенного подхода заключается в том, что он позволяет обеспечить защиту компьютерных сетей от сетевых атак, а также может быть использован как основа для построения систем классификации объектов.

Стиль изложения научных положений отличается лаконичностью и последовательностью. Автореферат грамотно написан и хорошо оформлен.

Выносимые на защиту научные результаты достаточно полно опубликованы в рецензируемых журналах и апробированы на научно-технических конференциях.

Однако содержание автореферата позволяет сделать несколько критических замечаний:

1. Не определены характеристики аномальных сетевых соединений, что затрудняет оценку степени эффективности разработанного модельно-методологического аппарата для их обнаружения.
2. Отсутствует сравнение разработанных предложений с моделями и алгоритмами, основанными на комбинированных подходах к обнаружению сетевых аномалий.

ул. Академика Павлова, д. 14-а, г. Санкт-Петербург, Россия, 197376
Телефон: (812) 438-76-54
Факс: (812) 438-76-54
E-mail: mail@spb.vega.su

ul. AcademicaPavlova, d.14-a, St. Petersburg, Russia, 197376
Phone: (812) 438-76-54
Fax: (812) 438-76-54
E-mail: mail@spb.vega.su

3. В автореферате цель исследования на страницах 4 и 7 сформулирована по-разному.

В целом, указанные недостатки существенно не снижают уровня научной и практической значимости проведенного исследования и общего положительного впечатления о работе.

Представленное диссертационное исследование представляет собой законченную научно-квалификационную работу, выполненную на актуальную тему и соответствующую критериям, изложенным в п. 9 абзац 2 «Положения о присуждении ученых степеней», предъявляемым к кандидатским диссертациям, в части решения научной задачи, имеющей значение для развития соответствующей отрасли знаний, а её автор, Браницкий Александр Александрович, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Ведущий научный сотрудник филиала акционерного общества «Концерн радиостроения «Вега» в г. Санкт-Петербурге, доктор технических наук, профессор

Игорь Николаевич Оков

Сведения о составителе отзыва:
Оков Игорь Николаевич, д.т.н., профессор, в.н.с. филиала акционерного общества «Концерн радиостроения «Вега» в г. Санкт-Петербурге.
Почтовый адрес: ул. Академика Павлова, д. 14а, г. Санкт-Петербург, 197376.
Тел.: 8(921)3238999
Электронная почта: okow1@mail.ru

ряю.
ала акционерного общества "Концерн
соналу

Юрий Владимирович Васин

"04" октября 2018 года

ул. Академика Павлова, д. 14-а, г. Санкт-Петербург, Россия, 197376
Телефон: (812) 438-76-54
Факс: (812) 438-76-54
E-mail: mail@spb.vega.su

ul. AcademicaPavlova, d.14-a, St. Petersburg, Russia, 197376
Phone: (812) 438-76-54
Fax: (812) 438-76-54
E-mail: mail@spb.vega.su