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».

Необходимость обработки сетевых потоков данных, а также их анализ на предмет наличия вредоносного содержимого в настоящее время приобретает все большую значимость. Такая потребность обосновывается регулярными и многочисленными отчетами крупных организаций о зафиксированных случаях сетевых аномалий, обусловленных реализацией компьютерных атак. Применение систем обнаружения атак (СОА) позволяет снизить количество таких сетевых угроз, а вместе с ними и возможные риски нарушения сетевой безопасности внутри организации. Поэтому исследуемая проблема является актуальной, а предлагаемый в диссертационной работе подход направлен на ее решение и позволяет повысить эффективность функционирования СОА.

В диссертации выполнено исследование применения комбинированного подхода с использованием сигнатурного анализа и методов вычислительного интеллекта для обнаружения аномальных сетевых соединений. С этой целью были получены четыре научных результата, обладающих новизной и практической значимостью. Это подтверждается выполненным анализом современного состояния затронутой темы, наличием шести работ, опубликованных автором в рецензируемых российских изданиях, и трех работ, индексируемых в международных изданиях Web of Science и Scopus, а также несколькими свидетельствами о регистрации программ для ЭВМ.

Среди выявленных в автореферате недостатков отмечаю следующие:

1. В автореферате не описано функциональное предназначение каждого компонента разработанной СОА (рис. 3), в частности, опущено описание интерпретатора и менеджера классификаторов.

2. В автореферате не приведено обоснование выбора сети Кохонена для внутреннего представления иммунных детекторов.

3. Из автореферата не ясно, что автор использовал в качестве сетевых параметров в событийно-ориентированном анализаторе трафика.

Указанные выше недостатки не влияют на положительное восприятие полученных автором результатов. Выполненное исследование является логически завершенным и содержит непротиворечивые выводы. На основе полученных экспериментальных результатов поставленная автором цель достигнута.

Считаю, что представленная в автореферате диссертационная работа соответствует требованиям п. 9 «Положения о порядке присуждения ученых степеней», предъявляемым ВАК при Минобрнауки России к диссертациям на соискание ученой степени кандидата технических наук, а ее автор, Браницкий Александр Александрович, заслуживает присуждения искомой ученой степени по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Профессор кафедры (автоматизированных систем специального назначения) Военной академии связи имени Маршала Совет М. Буденного, кандидат технических наук, доцент

В.С. Авраменко

«27» сентября 2018 г.

Сведения о составителе отзыва:
ФИО: Авраменко Владимир Семенович
Ученая степень: кандидат технических наук
Ученое звание: доцент
Должность: профессор кафедры Военной академии связи имени Маршала Советского Союза С.М. Буденного
Почтовый адрес: 194064, г. Санкт-Петербург, Тихорецкий пр., д. 3
Тел.: 8-812-2479437
Электронная почта: vsavr@yandex.ru