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»

Большинство систем обнаружения атак (СОА) построены на основе методов сигнатурного анализа, что накладывает на их функционирование существенное ограничение, которое заключается в невозможности обнаружения априори неизвестных модификаций сетевых атак. Для обнаружения неизвестных сетевых атак применяют эвристические алгоритмы, которые регистрируют аномальное функционирование сети и ее элементов. В настоящее время подобные алгоритмы реализуются на основе методов нейронных сетей, нечеткой логики и искусственных иммунных систем. Предлагаемые в диссертационной работе модель, алгоритм, методика и архитектура СОА для обнаружения аномальных сетевых соединений основаны на использовании гибридизации этих концепций, что позволяет улучшить классификационные характеристики комбинированных моделей и снизить время их обучения за счет их объединения в решающий классификатор. В связи с этим можно утверждать, что тема диссертационной работы Браницкого А.А. является актуальной.

В представленной работе решены следующие научно-технические задачи:

- на основе выполненного автором анализа сигнатурных и эвристических методов обнаружения сетевых атак выполнена разработка программных средств тестирования сетевых СОА и оценки их функциональных возможностей;
- разработана модель искусственной иммунной системы на основе эволюционного подхода для классификации сетевых соединений;

- разработан алгоритм генетико-конкурентного обучения сети Кохонена для обнаружения аномальных сетевых соединений;

- разработана методика иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений;

- предложена архитектура и разработано программное средство распределенной СОА;

- проведены эксперименты и выполнен их анализ по оценке эффективности предложенных алгоритмов.

Совокупность результатов решенных научно-технических задач позволила достигнуть поставленную цель исследования, а именно - повысить эффективность функционирования СОА.

Результаты, изложенные в тексте автореферата, опубликованы в шести журналах, рекомендованных ВАК, представлены на российских и международных конференциях, а также внедрены в учебный процесс нескольких образовательных учреждений. Кроме этого, практический вклад в исследуемую автором научную область подтверждается наличием свидетельств о регистрации программ для ЭВМ.

В представленном автореферате имеется следующие недостатки:

1. В предлагаемой методике не учитывается наличие лица, принимающего решения в функциональном контуре принятия решений.
2. В автореферате отсутствуют функциональные представления критериев и показателей, предназначенных для оценки эффективности СОА.
3. В автореферате не соблюдены правила оформления алгоритмов, что делает их представление менее наглядным.
4. Не приведены репрезентативности статистик, на основе которых оценивались показатели эффективности, их доверительные интервалы и доверительные вероятности.

Несмотря на указанные недостатки, считаю, что в работе Браницкого А.А. выполнено законченное исследование. Автореферат написан ясным научным языком. Диссертационная работа Браницкого А.А. удовлетворяет требованиям ВАК, указанным в п. 9

«Положения о порядке присуждения ученых степеней» и установленным для кандидатских диссертаций, а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Заместитель директора
научно-технического комплекса
прикладных информационных технологий
АО «Радиоавионика»
ехнических наук
__ С. Н. Попов
«2» октября 2018 г.

Подпись Попова С. Н. удостоверяю

Начальник отдела кадров
Е.А. Тимофеева

Начальник отде... 2018
Е.А. Тим...

Сведения о составителе отзыва:
ФИО: Попов Сергей Николаевич
Ученая степень: кандидат технических наук
Место работы: АО «Радиоавионика»
Должность: заместитель директора научно-технического комплекса прикладных информационных технологий
Почтовый адрес: г. Санкт-Петербург, Троицкий проспект, д. 4, литера Б, 190005
Телефон: 8(812)251-49-38