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 настоящее время задача обнаружения аномалий в сетевом трафике не теряет своей актуальности, поскольку из года в год наблюдается непрекращающийся рост нелегитимных действий в компьютерных сетях. Наличие событий, называемых аномальными сетевыми соединениями, отрицательно влияет на деятельность крупных организаций и обычных пользователей, что в итоге может приводить к серьезным финансовым потерям. Для выявления и предотвращения подобных ситуаций, связанных с сетевыми аномалиями, используются системы обнаружения атак, разработка которых требует совершенствования базовых механизмов их функционирования. Поэтому тема диссертационной работы Браницкого А.А. представляет собой важное направление исследований.

В диссертации ставится и успешно решается ряд частных задач, связанных с разработкой модельно-методического аппарата для обнаружения аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта. Особенность предложенного подхода заключается в построении различных схем комбинирования разнородных классификаторов, предназначенных для обнаружения сетевых атак, с поддержкой возможности добавления новых классификаторов или переобучения уже загруженных в систему классификаторов. Проведенные эксперименты, выполненные с использованием нескольких наборов данных, показали эффективность такого подхода и целесообразность его практического применения.

Стоит отметить некоторые недостатки, выявленные в автореферате:

1) из текста автореферата не вполне понятно, какие классы аномальных сетевых соединений рассматриваются в исследовании;

2) недостаточно убедительно показано, за счет чего удалось добиться ускорения процесса обработки сетевых пакетов и снижения ресурсопотребления в разработанной системе обнаружения атак.

Отмеченные недостатки не снижают научной ценности проведенного исследования.

Основные результаты диссертационной работы опубликованы в шести печатных изданиях, рекомендованных ВАК, представлены на международных и российских конференциях высокого уровня и внедрены в нескольких учебных заведениях.

Выводы:

1. Исследование обладает актуальностью, новизной и практической значимостью, а также отвечает требованиям, предъявляемым к кандидатским диссертациям в соответствии с п. 9 «Положения о порядке присуждения ученых степеней».

2. Браницкий Александр Александрович заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Профессор кафедры специальных информационных технологий
Федерального государственного казенного образовательного учреждения
высшего образования «Санкт-Петербургский университет Министерства
внутренних дел Российской Федерации»
доктор технических наук, профессор
Иванов Александр Юрьевич

«21» сентября 2018 г.

Сведения о составителе отзыва:
Иванов Александр Юрьевич, доктор технических наук, профессор,
Федеральное государственное казенное образовательное учреждение высшего образования «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации»
Почтовый адрес: г. Санкт-Петербург, ул. Летчика Пилютова, д. 1, 198206.
Телефон: (921) 757 8239
Адрес электронной почты: alexandr.y@mail.ru