ФАНО России
Федеральное государственное
бюджетное учреждение науки
Санкт-Петербургский институт
информатики и автоматизации
Российской академии наук
(СПИИРАН)

199178, Санкт-Петербург, 14 линия,
39
Телефон: (812)328-33-11
Факс: (812)328-44-50
E-mail: spiiran@iias.spb.su
http://www.spiiras.nw.ru
ОКПО 04683303, ОГРН
1027800514411
ИНН/КПП 7801003920/780101001

УТВЕРЖДАЮ
Директор
Санкт-Петербургского института
информатики и автоматизации
Российс[illegible]мии наук
професс[illegible]

А.Л. РОНЖИН
«14» июня 2018г.

ЗАКЛЮЧЕНИЕ
Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН)

Диссертация «Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта» выполнена в лаборатории проблем компьютерной безопасности Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук. В период подготовки диссертации диссертант Браницкий Александр Александрович работал в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук в лаборатории проблем компьютерной безопасности в должности младшего научного сотрудника, а также в ООО "НТЦ СевенТест" в должности инженера-программиста.

В 2012 году с отличием окончил математико-механический факультет Санкт-Петербургского государственного университета по специальности «Математическое обеспечение и администрирование информационных систем». В 2016 году с отличием окончил очную аспирантуру в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук. Справка о сдаче кандидатских экзаменов выдана 30 ноября 2016 года Федеральным государственным бюджетным учреждением науки Санкт-Петербургским институтом информатики и автоматизации Российской академии наук. Закончил диссертацию на соискание ученой степени кандидата технических наук.

Научный руководитель — Котенко Игорь Витальевич, доктор технических наук, профессор, главный научный сотрудник лаборатории проблем компьютерной безопасности Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук.

По результатам рассмотрения диссертации «Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта» принято следующее заключение:

Оценка выполненной соискателем работы

В диссертационной работе Браницкого Александра Александровича выполнен детальный анализ методов обнаружения сетевых атак, а также приведена их классификация. Разработаны модель, алгоритм и методика для обнаружения аномальных соединений в сетевом трафике с использованием комбинированного подхода, сочетающего сигнатурный анализ и методы вычислительного интеллекта. Выносимые на защиту результаты имеют важное практическое значение для построения систем обнаружения сетевых атак. Актуальность и востребованность выбранной темы подтверждаются постоянным и растущим интересом научно-исследовательского сообщества к решению задачи обнаружения аномальных сетевых соединений, который вызван необходимостью обеспечения безопасности сетевых ресурсов в условиях изменяющегося и обладающего разнообразными характеристиками сетевого трафика.

Личное участие соискателя в получении результатов, изложенных в диссертации.

Содержание диссертации и основные положения, выносимые на защиту, отражают персональный вклад автора в опубликованных работах. Подготовка к публикации полученных результатов проводилась совместно с Тимофеевым А.В. и Котенко И.В., причем вклад диссертанта был значительным. Представленные к защите результаты получены лично автором.

Достоверность результатов проведенных исследований.

Достоверность подтверждена аналитическим обзором исследований и программных прототипов в области обнаружения аномальных сетевых соединений, согласованностью теоретических результатов с результатами, полученными при проведении экспериментов, а также апробацией основных результатов в печатных трудах и докладах на российских и международных конференциях.

Научная новизна полученных результатов.

Научную новизну составляют разработанные (1) модель иммунной системы на базе эволюционного подхода для классификации сетевых соединений, которая отличается наличием двухуровнего алгоритма обучения иммунных

детекторов; (2) алгоритм генетико-конкурентного обучения сети Кохонена для обнаружения аномальных сетевых соединений, который дополнен введением различных стратегий генетической оптимизации весов «мертвых» нейронов; (3) методика иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений, которая позволяет задавать произвольную вложенность классификаторов и выполнять их «ленивое» подключение; (4) архитектура и программная реализация распределенной системы обнаружения атак, построенной на основе гибридизации методов вычислительного интеллекта и сигнатурного анализа и превосходящей другие открытые программные решения по скорости обработки пакетов и ресурсопотреблению.

Практическая значимость полученных результатов.
Разработанный модельно-методический аппарат реализован в виде вспомогательных библиотек машинного обучения и нескольких компонентов системы обнаружения атак (сетевые сенсоры, интерпретатор правил обучения классификаторов, менеджер классификаторов, балансировщик трафика и т.д.). Разработанный прототип может быть использован как для защиты компьютерных сетей, так и для решения других более общих задач, связанных с классификацией объектов.

Специальность, которой соответствует диссертация.
Работа соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность, и в частности п. 13 "Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности" паспорта соответствующей специальности.

Полнота изложения материалов диссертации в работах, опубликованных соискателем.
Основные результаты диссертации изложены в следующих работах в необходимой полноте:

1. **Браницкий, А.А. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейронечетких классификаторов / А.А. Браницкий, И.В. Котенко // Информационно-управляющие системы. – 2015. – 4 (77). – С. 69–77.**
2. **Браницкий, А.А. Построение нейросетевой и иммуноклеточной системы обнаружения вторжений / А.А. Браницкий, И.В. Котенко // Проблемы информационной безопасности. Компьютерные системы. – 2015. – № 4. – С. 23–27.**

3. **Браницкий, А.А. Анализ и классификация методов обнаружения сетевых атак / А.А. Браницкий, И.В. Котенко // Труды СПИИРАН. – 2016. – 2 (45). – С. 207–244.**
4. **Браницкий, А.А. Иерархическая гибридизация бинарных классификаторов для выявления аномальных сетевых соединений / А.А. Браницкий // Труды СПИИРАН. – 2017. – 3 (52). – С. 204–233.**
5. **Браницкий, А.А. Открытые программные средства для обнаружения и предотвращения сетевых атак / А.А. Браницкий, И.В. Котенко // Защита Информации. Инсайд. – 2017. – 2 (74). – С. 40–47.**
6. **Браницкий, А.А. Открытые программные средства для обнаружения и предотвращения сетевых атак (окончание) / А.А. Браницкий, И.В. Котенко // Защита Информации. Инсайд. – 2017. – 3 (75). – С. 58–66.**
7. Браницкий, А.А. Нейросетевой и иммуноклеточный подходы к распознаванию сетевых атак / А.А. Браницкий, А.В. Тимофеев // СПИСОК-2012. Материалы Всероссийской научной конференции по проблемам информатики. 25–27 апреля 2012 г. Санкт-Петербург. Т. 6. – Изд. "ВВМ", СПбГУ, 2012. – С. 335–340.
8. Branitskiy, A. Network attack detection based on combination of neural, immune and neuro-fuzzy classifiers / A. Branitskiy, I. Kotenko // In Proceedings of the 18th IEEE International Conference on Computational Science and Engineering (IEEE CSE2015). – IEEE. Oct. 2015. – Pp. 152–159.
9. Branitskiy, A. Hybridization of computational intelligence methods for attack detection in computer networks / A. Branitskiy, I. Kotenko // Journal of Computational Science. – 2017. – Vol. 23. – Pp. 145–156.
10. Branitskiy, A. Network Anomaly Detection Based on an Ensemble of Adaptive Binary Classifiers / A. Branitskiy, I. Kotenko // In Proceedings of International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. – Springer. 2017. – Pp. 143–157.

Диссертация «Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта» Браницкого Александра Александровича рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 05.13.19 — Методы и системы защиты информации, информационная безопасность. Заключение принято на расширенном семинаре Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук. Присутствовало на семинаре 30 чел. Результаты голосования: «за» — 30 чел., «против» — 0 чел., «воздержалось» — 0 чел., протокол №1 от 26.04.2018 г.

Председатель расширенного семинара — д.т.н., в.н.с., проф. И.Б. Саенко

Секретарь расширенного семинара — к.т.н., зав.лаб. Р.Ш. Фахрутдинов