**Отзыв**

официального оппонента, доктора технических наук,
Шерстюка Юрия Михайловича
на диссертационную работу Браницкого Александра Александровича на тему «Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта», представленную на соискание ученой степени кандидата технических наук
по специальности 05.13.19
«Методы и системы защиты информации, информационная безопасность»

## 1. Актуальность темы диссертационной работы

В настоящее время наблюдается быстрый рост компьютерных сетей, одновременно с этим увеличивается и разнообразие классов сетевых атак. Такие условия требуют разработки специальных программных средств, предназначенных для пассивного прослушивания сетевого трафика и обнаружения в нем аномалий, а именно сетевых систем обнаружения атак (СОА). Подходы, используемые при построении этих систем, условно можно разделить на сигнатурные и эвристические. В случае реализации сигнатурной СОА поиск вредоносной сетевой активности осуществляется на основе правил, точно идентифицирующих тот или иной тип сетевой угрозы. В случае реализации эвристической СОА появляется возможность обнаружения неизвестных атак за счет использования алгоритмов, выявляющих отличия от шаблонов нормального поведения в сети (к примеру, статистические методы обнаружения аномалий) или выполняющих адаптивную настройку некоторой вычислительной структуры (к примеру, алгоритмы обучения нейронной сети). Каждый из этих подходов имеет свои преимущества и недостатки. Чтобы совместить сильные стороны этих подходов и устранить их недостатки, используют прием их комбинирования, который по-прежнему остается не до конца исследованным в области построения сетевых СОА. Применение т.н. гибридных СОА позволяет снизить количество пропусков сетевых атак на критически важные секторы деятельности человека за счет многократного анализа передаваемых по сети групп пакетов, объединенных на сетевом и транспортном уровнях модели OSI в сетевые соединения.

Поэтому разработанный в данном диссертационном исследовании подход, который базируется на комбинировании (гибридизации) разнородных бинарных классификаторов вычислительного интеллекта (ВИ) и сигнатурном анализе, является перспективным, а рассматриваемая тема является актуальной.

## 2. Структура диссертационной работы

Диссертационная работа состоит из введения, трех глав, заключения и пяти приложений и включает 305 страниц машинописного текста. Структура диссертационной работы выглядит логичной и цельной, название глав и разделов соответствует выбранной теме исследования.

Во введении описана актуальность темы диссертационного исследования, поставлена цель и сформулированы задачи. В первой главе выполнен анализ проблемы обнаружения сетевых атак, сформулирован список требований, предъявляемых к сетевым СОА, выполнена постановка задачи исследования. Во второй главе представлены первые три научных результата, выносимые на защиту. Третья глава посвящена разработке архитектуры СОА (четвертому результату) и экспериментальной оценке эффективности разработанной СОА. В заключении перечислены научные результаты и рекомендации по применению разработанного модельно-методического аппарата для построения СОА. В приложениях выполнен анализ нескольких СОА с открытым исходным кодом, приведены примеры обнаружения сетевой атаки типа "подбор пароля" при помощи каждой СОА, представлены грамматика интеллектуального ядра классификации объектов, иллюстративный материал по результатам экспериментов и копии актов о внедрении результатов диссертационной работы.

**3. Научная новизна полученных результатов**

1) Разработана модель искусственной иммунной системы на базе эволюционного подхода для классификации сетевых соединений. Модель, в отличие от существующих, характеризуется наличием двухуровневого алгоритма обучения детекторов и возможностью автоматического вычисления порога их активации. Данная модель позволяет повысить эффективность функционирования СОА и снизить частоту возникновения конфликтных случаев классификации сетевых соединений.
2) Разработан алгоритм генетико-конкурентного обучения сети Кохонена для обнаружения аномальных сетевых соединений. Алгоритм отличается от существующих введением нескольких стратегий генетической оптимизации весов нейронов в процесс обучения сети Кохонена. Наличие этого алгоритма в ядре СОА позволяет снизить время настройки ее детекторов, представленных сетями Кохонена и предназначенных для обнаружения аномальных сетевых соединений.
3) Разработана методика иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений. Методика, в отличие от известных, ориентирована на многоуровневый анализ вектора признаков сетевых соединений за счет наличия алгоритма каскадного обучения классификаторов и разделения задач, связанных с обнаружением сетевых атак, между сенсорами и коллектором. Роль сенсоров — первичный сбор данных о признаках сетевых соединений и выполнение сигнатурного анализа содержимого отдельных и дефрагментированных пакетов, роль коллектора — анализ сетевых соединений при помощи комбинированных классификаторов. Использование предложенной методики в ядре СОА позволяет скомплексировать такие разнородные средства обнаружения аномальных сетевых соединений, как сигнатурный анализ и методы ВИ.

4) Разработана архитектура распределенной СОА, построенной на основе гибридизации методов ВИ и сигнатурного анализа. Предложенная архитектура, в отличие от известных, поддерживает «горячую» вставку нового исполняемого кода, содержащего функционирование и структуру классификатора, характеризуется наличием интерпретатора на основе контекстно-свободной грамматики с левосторонней рекурсией для создания обучающих выборок и правил формирования входных сигналов классификаторов, а также обладает поддержкой оригинальной методики иерархической гибридизации бинарных классификаторов с приложением к обнаружению аномальных сетевых соединений.

**4. Обоснованность и достоверность**

Обоснованность научных положений, выводов и рекомендаций достигается за счет:

- выполнения тщательного анализа состояния исследований в области обнаружения аномальных сетевых соединений;
- корректности используемого математического аппарата при постановке и решении задачи.

Достоверность научных положений, выводов и рекомендаций подтверждается:

- соответствием теоретических результатов результатам, полученным в ходе проведения экспериментов;
- наличием актов о внедрении результатов диссертационной работы в учебный процесс нескольких учебных заведений;
- публикацией в ведущих рецензируемых изданиях российского и международного уровней;
- апробацией результатов на нескольких научных конференциях.

**5. Практическая значимость**

Использование разработанной методики позволит повысить эффективность функционирования СОА за счет комбинирования сигнатурного анализа и адаптивных классификаторов ВИ. Разработанный модельно-методический аппарат может быть использован для обнаружения аномальных сетевых соединений и для решения других более общих задач, связанных с классификацией многомерных векторов признаков объектов.

**6. Замечания по диссертационной работе**

1) На стр. 112 в разделе 2.5 диссертационной работы не обосновано использование формулы, задающей гибридное правило (смесь голосования большинством и голосования max-wins) для объединения групп бинарных классификаторов в единый классификатор.
2) Ограничением в применении разработанной СОА является ее узкая ориентация на функционирование в компьютерных сетях, выполняющих передачу сетевых пакетов по протоколу IPv4. С учетом возрастающей

распространенности обновленной версии IP, а именно IPv6, стоило указать необходимость поддержки этого протокола в ядре СОА среди перспектив дальнейшей разработки темы (стр. 181).

3) На стр. 246 в приложении А.9 диссертационной работы были исследованы атаки, характерные только для сигнатурных СОА (атаки со скрытием и со вставкой), однако не выполнен анализ атак, направленных на искажение обучающих выборок и свойственных нейросетевым СОА (атаки «отравления» классификационной модели).

Следует отметить, что выявленные замечания не снижают положительную оценку диссертационного исследования и не влияют на новизну, практическую значимость, обоснованность и достоверность полученных в нем результатов.

**7. Вывод**

Диссертационная работа Браницкого А.А. обладает новизной и практической значимостью полученных результатов, представляет собой единолично написанную им научно-квалификационную работу, в которой выполнено решение важной научно-технической задачи, заключающейся в разработке модельно-методического аппарата для обнаружения аномальных сетевых соединений на основе гибридизации методов ВИ. Полученные результаты соответствуют паспорту специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность». Диссертационная работа выполнена в соответствии с критериями п. 9 «Положения о присуждении ученых степеней», утвержденного постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 г., предъявляемыми к кандидатским диссертациям. Тем самым автор диссертационного исследования, Браницкий Александр Александрович, заслуживает присуждения искомой ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная

Официальный оп
доктор техническ Шерстюк Юрий Михайлович

17.09.2018

Сведения о соста
ФИО: Шерстюк Юрий Михайлович
Ученая степень: доктор технических наук
Ученое звание: доцент
Место работы: АО «НИИ «Рубин»
Должность: заместитель генерального конструктора
Почтовый адрес: 194100, Санкт-Петербург, ул. Кантемировская, д. 5
Телефон (рабочий): +7(812)670-89-89
Адрес электронной почты: yusher@iitc.ru