ОТЗЫВ

на автореферат диссертации Браницкого Александра Александровича «Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта», представленной к защите на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

В диссертационном исследовании, кратко представленном в данном автореферате, рассматривается решение важной проблемы, которая является одной из ключевых в области информационной безопасности и заключается в совершенствовании систем обнаружения атак (СОА). Современные сетевые атаки отличаюстя изощренностью, высокоуровневой направленностью, адаптивностью и «интеллектуальностью» при обходе механизмов обнаружения. Поэтому диссертационное исследование, направленное на решение задачи обнаружения аномальной сетевой активности на логическом уровне с комбинированием подходов, несомненно актуально. Вопрос обеспечения сетевой безопасности особенно остро возникает в крупных организациях, которые имеют распределенную структуру, включающую несколько сотен или тысяч хостов. Поддержка непрерывного процесса обнаружения сетевых аномалий в столь крупных компьютерных сетях существенно затрудняется с учетом разнообразия типов сетевого оборудования и семейств операционных систем. Для решения этой задачи необходимо применять современные инструментальные средства (например, высокоскоростные драйверы захвата сетевого трафика для построения анализаторов СОА, параллельные алгоритмы обработки сетевого трафика, адаптированные под исполнение на графических видеокартах) и гибридные подходы (в т.ч. такие традиционные подходы, как сигнатурный анализ, и такие эвристические подходы, как нейронные сети),

которые позволят достичь оперативного анализа сетевого трафика и наилучшего покрытия неизвестных вариаций сетевых угроз.

Научная новизна выносимых на защиту положений не вызывает сомнений: в частности разработанный модельно-методический аппарат отличается от известных возможностью гибкого построения (за счет «горячего» подключения новых классификаторов и независимости разработанной структуры от базовых классификаторов) многоуровневых схем комбинирования разнородных решателей и наличием оригинального алгоритма обхода дерева классификаторов с приложением к обнаружению аномальных сетевых соединений.

Достоверность полученных результатов достигается путем проведения множества различных экспериментов с несколькими наборами данных, согласованностью экспериментальных и теоретических результатов, а также публикацией полученных результатов в журналах, реферируемых ВАК РФ и индексированных в международных системах цитирования Web of Science и Scopus.

Практическая значимость разработанного подхода заключается в возможности его реализации в виде компонентов СОА для защиты компьютерных сетей и подтверждается несколькими свидетельствами о регистрации программ для ЭВМ.

Среди замечаний, выявленных в тексте автореферата, стоит выделить следующие. В автореферате недостаточно раскрыт вопрос целесообразности использования протокола RPC/SSL в качестве связующего звена между сенсорами и коллектором СОА. На стр. 7 в начале последнего абзаца автор указывает, что формулы (1) и (2) описывают разработанную модель искусственной имунной системы, однако из них не видно тех особенностей, которые выделяют её из существующих моделей. Кроме того, недостаточно освещены механизмы межъязыкового взаимодействия плагинов внутри

интеллектуального ядра классификации объектов, а также недостаточно рассмотрены возможности внедрения вредоносного кода в ядро СОА за счет загрузки нелегитимных плагинов.

Приведенные замечания носят частный характер и не оказывают влияния на положительную оценку выполненной соискателем работы. Считаю, что данная диссертационная работа удовлетворяет требованиям п. 9 «Положение о присуждении учёных степеней», предъявляемым к кандидатским диссертациям, а её автор, Браницкий Александр Александрович, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Доцент кафедры «Информатика и информационная безопасность» Федерального государственного бюджетного образовательного учреждения высшего образования «Петербургский государственный университет путей сообщения Императора Александра I»,
кандидат технических наук, доцент

Диасамидзе Светлана Владимировна

190031, Россия, г. Санкт-Петербург,
Московский пр., д. 9
тел. 8 (812) 310-34-72
e-mail: sv.diass99@yandex.ru

"19" 09 2018