ОТЗЫВ

официального оппонента, доктора технических наук, Комашинского Владимира Ильича 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»

Актуальность темы диссертационной работы

Увеличение количества сетевых компьютеров и расширение вычислительных сетей происходит на фоне быстрого увеличения объемов передаваемых данных и проблем обеспечения информационной безопасности. В этих условиях поиск аномалий сетевых соединений должен производиться быстро и с высокой степенью достоверности. Для решения этой задачи в настоящее время широко применяются сетевые системы обнаружения атак (СОА), осуществляющие анализ сетевого трафика между хостами в интересах обнаружения вредоносной сетевой активности. В основе большинства существующих СОА применяется сигнатурный анализ как один из наиболее распространенных подходов, который хорошо зарекомендовал себя при поиске шаблонных аномальных действий. Вместе с тем недостатками такого решения являются ограничения в обнаружении модифицированных вариантов известных атак.

Поэтому предложенный в диссертационной работе новый подход, основанный на комбинировании разнородных классификаторов вычислительного интеллекта (ВИ) и сигнатурного анализа, позволяющий выявлять скрытые закономерности в сетевых потоках данных, является **актуальным и практически востребованным**.

Научная новизна полученных в диссертации результатов заключается в следующем:

1. Предложена модель искусственной иммунной системы, основанная на применении эволюционного подхода для классификации сетевых соединений. Модель отличается от существующих наличием двухуровневого алгоритма обучения и процедуры автоматического вычисления порога активации иммунных детекторов, что позволяет повысить достоверность детектирования сетевых атак.
2. Разработан алгоритм генетико-конкурентного обучения искусственной нейронной сети Кохонена для обнаружения аномальных сетевых соединений. Предложенный алгоритм отличается от существующих наличием нескольких стратегий генетической оптимизации весов искусственных нейронов. Поддержка данного алгоритма в СОА позволяет снизить время настройки сети Кохонена, обученной для распознавания аномальных сетевых соединений.
3. Синтезирована методика иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений. Методика отличается от известных возможностью задания произвольной вложенности классификаторов друг в друга и их «ленивым» подключением благодаря наличию алгоритма каскадного обучения узлов, это позволяет в контексте обнаружения аномальных сетевых соединений объединить разнородные средства обнаружения аномальных сетевых соединений, включая методы ВИ и сигнатурный анализ, и тем самым создать основу для построения гибридной СОА.
4. Исследована архитектура распределенной СОА, построенной на основе гибридизации методов ВИ и сигнатурного анализа. Архитектура отличается от известных возможностью «горячей» вставки исполняемого кода, содержащего функционирование классификатора, без останова системы, наличием интерпретатора для написания собственных сценариев, задающих структуры и правила обучения

классификаторов и поддержкой оригинальной методики иерархической гибридизации бинарных классификаторов.

Обоснованность и достоверность приведенных в диссертационной работе научных положений, выводов и рекомендаций подтверждается:

- выполнением детального анализа исследований в области обнаружения аномальных сетевых соединений;
- согласованностью теоретических и экспериментальных результатов;
- актами о внедрении результатов диссертационного исследования;
- публикацией в ведущих рецензируемых изданиях.

Практическая значимость полученных результатов состоит в том, что они могут быть использованы для обеспечения безопасности хостов, объединенных локальной компьютерной сетью и находящихся в критически важных организациях. Теоретические результаты могут применяться при построении таких компонентов СОА, как адаптивных модулей на основе методов ВИ. Это подтверждается наличием трех свидетельств о государственной регистрации программ для ЭВМ.

Диссертационная работа включает 305 страниц и состоит из введения, трех глав, заключения и пяти приложений. Список литературы содержит 213 наименований. Диссертация написана строгим научным языком, хорошо структурирована и представляет собой законченную научно-квалификационную работу.

По диссертационной работе имеются некоторые замечания:

1. Применение классификаторов ВИ рассматривается в контексте обнаружения сетевых атак, относящихся только к сетевому и транспортному уровням модели OSI. Однако сетевые атаки более низкого уровня (такие как ARP-спуфинг) или более высокого уровня (такие как атаки переполнения буферов сетевых приложений) не принимаются во внимание.

2. В диссертационной работе не в полной мере рассмотрены атаки, которым может быть подвержена сама СОА, например состязательные атаки.
3. В эксперименте 10, представленном в разделе 3.4, проводится сравнение характеристик разработанной СОА с характеристиками других сетевых СОА. Сравнение осуществляется в рамках одной вычислительной платформы, при этом не совсем ясно, сохранится ли преимущество разработанной СОА перед остальными при их переносе на другие платформы.
4. В разделе 3.2 не обоснован выбор некоторых технологий (flex, bison, rpcgen), использованных при разработке СОА.

Вместе с тем отмеченные недостатки не снижают качества диссертационного исследования.

Заключение

1. Диссертационная работа Браницкого А.А. является законченной научно-квалификационной работой, содержит полный цикл исследований, обладает новизной и практической значимостью результатов.
2. В диссертационной работе Браницкого А.А. решена важная научно-техническая задача, которая заключается в разработке модельно-методического аппарата для обнаружения аномальных сетевых соединений на основе гибридизации методов ВИ.
3. Диссертационная работа отвечает требованиям п. 9 «Положения ВАК Минобрнауки РФ», предъявляемым ВАК Министерства науки и образования России к кандидатским диссертациям; полученные в диссертационной работе результаты соответствует паспорту специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».
4. Браницкий Александр Александрович заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19

«Мето[redacted]ормации, информационная безопа[redacted]

Официальны[redacted]

доктор техни[redacted]ашинский Владимир Ильич

Сведения о [redacted]

ФИО: Комаг[redacted]

Ученая степ[redacted]: доктор технических наук

Ученое звание: доцент

Место работы: Институт проблем транспорта Российской академии наук им. Н.С. Соломенко

Должность: заместитель директора по научной работе

Почтовый адрес: 199178, г. Санкт-Петербург, 12-я линия ВО, д. 13

Телефон (рабочий): +7(812)323-29-54

Адрес электронной почты: kama54@rambler.ru