ИНТЕЛТЕХ INTELTECH

Публичное акционерное общество «Информационные телекоммуникационные технологии» (ПАО «Интелтех»)

УТВЕРЖДАЮ

ıерального директора

учной работе,

:, доцент

И.А. Кулешов

_ 2018 г.

ОТЗЫВ

ведущей организации ПАО «Интелтех» на диссертацию Браницкого Александра Александровича «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

В диссертационном исследовании решается задача разработки модельно-методического аппарата для обнаружения аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта (ВИ).

В условиях постоянного совершенствования навыков атакующих и роста вредоносного программного обеспечения (ПО), генерирующего аномальный трафик, администраторам безопасности требуется выполнять проверку множества узлов, объединенных в локальную компьютерную сеть. Для решения этой задачи используются сетевые системы обнаружения атак (СОА). Разнообразие компьютерных атак и их непрерывный рост усложняют

разработку подобных средств. Для обеспечения безопасности сетевых узлов на сетевом и транспортном уровнях модели OSI в СОА должен быть реализован механизм сборки потоков сетевых пакетов в сетевые соединения. Характеристики, свойственные сетевым соединениям, могут быть использованы в качестве набора признаков для обучения адаптивных классификаторов, к примеру, классификаторов на основе вычислительного интеллекта.

Наличие аномалий в компьютерных сетях отрицательно влияет на функционирование сетевых узлов, снижает полезную пропускную способность сетевого канала и может приводить к отказу сетевого оборудования, для устранения которого потребуется значительное время. Кроме того, успешные атаки могут приводить к потере критически важной информации с серьезными последствиями для организаций. Поэтому рассматриваемая в диссертационной работе тема является актуальной.

Структура диссертационной работы

Диссертационная работа состоит из введения, трех разделов, заключения и пяти приложений.

Во *введении* обоснована актуальность рассматриваемой в диссертации темы исследования, определена цель, сформулированы задачи, решение которых необходимо выполнить для достижения поставленной цели. Показаны научная новизна и практическая значимость работы. Приведено краткое описание полученных научных результатов.

Первая глава содержит анализ проблемы обнаружения аномальных сетевых соединений. В главе представлены анализ и классификация методов обнаружения сетевых атак. Приведена классификация СОА и общая архитектура сетевой распределенной СОА. Сформулирован список требований, предъявляемых к СОА. Выполнена постановка задачи исследования, заключающаяся в разработке модельно-методического аппарата для обнаружения аномальных сетевых соединений на основе гибридизации методов ВИ. Сформулирована цель исследования, состоящая в повышение

эффективности функционирования СОА через снижение значения функционала эмпирического риска на объектах контрольной выборки.

Во *второй главе* выполнен анализ искусственных иммунных систем и нескольких исследовательских прототипов СОА, построенных на основе искусственных иммунных систем. Представлены разработанные модель искусственной иммунной системы, алгоритм генетико-конкурентного обучения сети Кохонена, методика иерархической гибридизации бинарных классификаторов с приложением к обнаружению аномальных сетевых соединений.

Третья глава посвящена разработке архитектуры сетевой распределенной СОА, и описанию ее программной реализации. Выполнено сравнение характеристик производительности разработанной СОА с характеристиками производительности других открытых СОА, обосновано выполнение предъявленных к СОА требований. Представлены предложения по применению разработанного модельно-методического аппарата для построения СОА.

Заключение содержит перечисление основных научных результатов и рекомендаций по применению разработанного модельно-методического аппарата для построения сетевых СОА.

В *приложениях* выполнен анализ пяти открытых СОА, произведено их тестирование с целью проверки способности к обнаружению атак со скрытием и со вставкой. Представлены примеры обнаружения сетевой атаки типа «подбор пароля» средствами каждой СОА, грамматика интеллектуального ядра классификации объектов, результаты экспериментов и копии актов о внедрении результатов диссертационной работы.

Научная новизна исследования и полученных результатов, выводов и рекомендаций, сформулированных в диссертации

Научная новизна диссертационного исследования заключается в следующем:

разработанная *модель* искусственной иммунной системы на базе эволюционного подхода для классификации сетевых соединений *отличается* от известных наличием двухуровневого алгоритма ее обучения, механизмом разрешения конфликтных случаев классификации, процедурой автоматического вычисления порога активации иммунных детекторов, а также универсальностью структуры для их представления. Для учета свойств динамического непостоянства сетевого трафика в основу функционирования данной модели заложены механизмы постоянного обновления иммунных детекторов в течение различных этапов созревания (жизненного цикла) и их переобучения с использованием расширяющегося набора аномальных сетевых записей;

разработанный *алгоритм* генетико-конкурентного обучения сети Кохонена для обнаружения аномальных сетевых соединений *дополнен* введением различных стратегий генетической оптимизации весовых коэффициентов «мертвых» нейронов, расположенных на выходном слое сети. Предложенная стохастическая оптимизация позволяет сократить количество эпох обучения сети Кохонена при достижении заданного максимального значения ошибки векторного квантования. Тем самым разработанный алгоритм позволяет снизить время адаптации СОА к новым сетевым аномалиям в режиме непосредственного анализа трафика;

разработанная *методика* иерархической гибридизации бинарных классификаторов (детекторов) для обнаружения аномальных сетевых соединений *отличается* от известных возможностью задания произвольной вложенности классификаторов друг в друга и их «ленивым» подключением благодаря наличию алгоритма каскадного обучения узлов. Особенность методики заключается в возможности гибкого объединения детекторов для построения единого верхнеуровневого классификатора при помощи различных низкоуровневых схем их комбинирования и агрегирующих композиций. Применение данной методики позволяет объединить разнородные средства обнаружения аномальных сетевых соединений,

включая методы ВИ и сигнатурный анализ, и создать основу для построения гибридной СОА;

разработанная *архитектура* распределенной СОА, построенной на основе гибридизации методов ВИ и сигнатурного анализа, *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, а также поддержкой оригинальной методики иерархической гибридизации детекторов. За счет наличия механизмов балансировки трафика и преаллокации списка записей сетевых соединений данная СОА, в отличие от других программных решений, обладает существенно более высокой скоростью обработки сетевых потоков и более низким ресурсопотреблением.

Обоснованность и достоверность научных положений

Обоснованность и достоверность изложенных в диссертационной работе научных положений обеспечивается выполнением детального анализа состояния исследований в области обнаружения аномальных сетевых соединений, подтверждается согласованностью теоретических результатов с экспериментальными результатами, а также публикацией в ведущих рецензируемых журналах российского и международного уровня.

Теоретическая и практическая значимость результатов

Разработанные компоненты предназначены для повышения корректности детектирования сетевых атак, что позволит обеспечить необходимый уровень защищенности информационных ресурсов. Разработанная методика иерархической гибридизации бинарных классификаторов позволит объединить разнородные средства обнаружения сетевых атак, включая различные адаптивные методы и сигнатурный анализ, для создания гибридной СОА. Поскольку в качестве минимальной единицы классификации сетевых атак используются адаптивные детекторы, проектирование СОА можно рассматривать в стиле «снизу-вверх»: вначале

ее ядро приспосабливается под выявление отдельных типов атак, затем оно строит правила (комбинирует детекторы, разрешает конфликтные ситуации, формирует входные сигналы для верхнеуровневых классификаторов, выполняет обход дерева классификаторов) для соотнесения подозрительного сетевого соединения к тому или иному классу. Разработанный модельно-методический аппарат может быть использован как для защиты компьютерных сетей, так и для решения других более общих задач, связанных с классификацией объектов.

Соответствие паспорту специальности

Полученные результаты соответствуют паспорту 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».

Рекомендации по использованию результатов диссертации

Полученные в диссертационной работе результаты и выводы могут быть использованы на предприятиях, в организациях и учреждениях государственного и банковского сектора, в которых необходимо обеспечивать высокий уровень безопасности в компьютерных сетях, а также в учебном процессе вузов, ведущих подготовку специалистов информационной безопасности, например, в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербургском национальном исследовательском университете информационных технологий, механики и оптики и др. с целью разработки компонентов СОА и проведения лабораторных работ.

Замечания и недостатки по диссертации

В качестве замечаний и недостатков диссертации можно отметить:

1. Применяемый во втором научном положении генетический алгоритм характеризуется ресурсоемкими вычислениями, что может негативно

сказываться на производительности всей системы в целом. Данный факт имеет существенное значение при разработке адаптивных модулей СОА, однако не отражен в тексте диссертации.

2. В диссертационной работе не обоснован выбор набора из восьми показателей эффективности классификаторов. Некоторые из этих показателей, такие как показатель переобученности при классификации, по нашему мнению, являются избыточными.

3. Часть первого раздела главы 2 содержит описание элементов естественной иммунной системы и особенностей ее функционирования. Считаем, что данный материал имеет косвенное отношение к решению рассматриваемой научной задачи и может быть исключен из текста диссертации без потери смыслового содержания ее оставшейся части.

4. В разделе 3.2 представлен алгоритм каскадного обучения дерева классификаторов, однако не приведена оценка его сложности. Для СОА, в основе функционирования которой используется данный алгоритм, этот показатель является особенно важным.

5. Для проведения экспериментов использовалось несколько наборов данных, содержащих бинарные дампы сетевого трафика. Однако в работе недостаточно подробно раскрыто описание процесса формирования на их основе обучающих наборов данных, используемых для настройки адаптивных классификаторов, не обоснован выбор мощности обучающей выборки для искусственной иммунной системы и других адаптивных классификаторов на основе ВИ.

Однако, отмеченные недостатки не носят принципиального характера, не ставят под сомнение основные результаты полученные автором самостоятельно и не снижают общей высокий теоретический и прикладной уровень работы.

Автореферат соответствует основным результатам, изложенным в диссертации и достаточно полно отражает ее основное содержание, новизну, теоретическую и практическую значимость. Оформление диссертационной работы и автореферата соответствует ГОСТ 7.0.11–2011.

ВЫВОД: представленная диссертация «Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта» является законченной научно-квалификационной работой, в которой решена актуальная и значимая научно-техническая задача — разработка модельно-методического аппарата для обнаружения аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта, соответствует критериям раздела II «Положения о присуждении ученых степеней» (утвержденного постановлением Правительства Российской Федерации от 24.09.2013 г. № 842.), предъявляемым к кандидатским диссертациям, а ее автор, Браницкий Александр Александрович, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Отзыв обсуждён и одобрен на заседании теоретической секции НТС ПАО «Интелтех». Протокол № 15 от 20.07.2018 г.

Отзыв подготовили:

Ученый секретарь ПАО «Инте

доктор технических наук, про Павел Александрович Будко

Заместитель начальника отдел

кандидат технических наук, до Дмитрий Владиславович Салюк

Начальник отдела

кандидат технических наук Михаил Васильевич Бакаев

Подписи ученого секретаря ПАО «Интелтех» доктора технических наук, профессора Будко Паввла Александровича, заместителя начальника отдела кандидата технических наук, доцента Салюка Дмитрия Владиславовича и начальника отдела кандидата технических наук Бакаева Михаила васильевича ЗАВЕРЯЮ

Нача бедева Елена Оттовна