На правах рукописи

Браницкий Александр Александрович

ОБНАРУЖЕНИЕ АНОМАЛЬНЫХ СЕТЕВЫХ СОЕДИНЕНИЙ НА ОСНОВЕ ГИБРИДИЗАЦИИ МЕТОДОВ ВЫЧИСЛИТЕЛЬНОГО ИНТЕЛЛЕКТА

Специальность 05.13.19 —
«Методы и системы защиты информации,
информационная безопасность»

Автореферат
диссертации на соискание учёной степени
кандидата технических наук

Санкт-Петербург — 2018

Работа выполнена в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук

Научные руководители: доктор технических наук, профессор **Тимофеев Адиль Васильевич**,
доктор технических наук, профессор **Котенко Игорь Витальевич**

Официальные оппоненты: **Комашинский Владимир Ильич,**
доктор технических наук, доцент,
Институт проблем транспорта Российской академии наук им. Н.С. Соломенко,
заместитель директора по научной работе

Шерстюк Юрий Михайлович,
доктор технических наук, доцент,
АО «НИИ «Рубин»,
заместитель генерального конструктора

Ведущая организация: Публичное акционерное общество «Информационные телекоммуникационные технологии»

Защита состоится «09» октября 2018 г. в 14 часов 00 минут на заседании диссертационного совета Д 002.199.01 при Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук по адресу: 199178, Россия, Санкт-Петербург, 14 линия, дом 39.

С диссертацией можно ознакомиться в библиотеке и на сайте Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, http://www.spiiras.nw.ru.

Автореферат разослан «___» _____ 2018 года.

Ученый секретарь
диссертационного совета
Д 002.199.01, канд. техн. наук

Зайцева
Александра
Алексеевна

Общая характеристика работы

Актуальность темы. Разработка системы обнаружения атак (СОА) является одним из приоритетных направлений в области информационной безопасности. Важность решения этой задачи обусловливается постоянным увеличением и разнообразием компьютерных сетевых угроз, реализация которых может приводить к серьезным финансовым потерям в различных организациях. Согласно статистическим данным „Лаборатории Касперского“ в первом квартале 2017 г. было выявлено и отражено более 479 млн. компьютерных атак, в то время как за аналогичный период 2018 г. этот показатель уже превысил величину в 796 млн. атак. Подобный рост атакующих действий с каждым годом требует задействования существенно больших сил и временных затрат со стороны администраторов и аналитиков безопасности. В компаниях, вовлеченных в производство критически важной продукции, для поддержания безопасности корпоративных сетевых ресурсов расходуются крупные финансовые и материальные средства, направленные на содержание специального оборудования в виде компонентов СОА и обслуживающего его персонала. Для обеспечения корректной интерпретации передаваемых в пакетах данных необходимо выполнять их сборку в минимальный логический поток — сетевое соединение, что позволит оперировать более высокоуровневыми характеристиками сетевого трафика для выявления аномалий, свойственных сетевому и транспортному уровням модели OSI.

Для обнаружения сетевых атак могут применяться как сигнатурные механизмы поиска шаблонных аномальных действий, так и эвристические (статистические, нейросетевые, иммунные и пр.) подходы. В случае сигнатур решение задачи сводится к реализации процедуры, выполняющей проверку вхождения заданной байтовой последовательности внутри содержимого сетевых пакетов. Недостатками такого решения являются сложность создания репрезентативного набора с подобными записями и ограничение в обнаружении модифицированных вариантов известной атаки. Напротив, эвристические подходы позволяют выявлять скрытые закономерности в анализируемых сетевых потоках. Именно эта особенность объясняет их широкую популярность в научно-исследовательском сообществе и играет ключевую роль при выборе и проектировании ядра СОА. С другой стороны, в основе функционирования большинства коммерческих и открытых программных решений преобладает подход, который базируется на сигнатурном сопоставлении с образцом и характеризуется минимальным числом ложных срабатываний. Для сохранения преимуществ обоих подходов используется прием их комбинирования, который по-прежнему остается не в полной мере исследованным. Поэтому задача обнаружения аномальных сетевых соединений является актуальной, а предлагаемый в настоящем диссертационном исследовании модельно-методический аппарат, использующий комбинирование (гибридизацию) разнородных методов вычислительного интеллекта (ВИ) и сигнатурного анализа, направлен на ее решение. Область ВИ охватывает исследование биологически инспирированных моделей (нейронных сетей, нечеткой логики, эволюционных вычислений и т.д.), направленных на обработку низкоуровневых данных об объекте без использования экспертных знаний. Под термином «гибридизация» понимается комбинирование разнородных решателей в единую систему классификации объектов.

Степень разработанности темы. Вопросу обнаружения аномальных сетевых соединений посвящены работы как отечественных исследователей С.В. Безобразова, А.К. Большева, В.И. Васильева, Д.Ю. Гамаюнова, В.А. Головко, П.Д. Зегжды, И.В. Котенко, А.В. Лукацкого, О.Б. Макаревича, С.А. Петренко, В.В. Платонова, О.И. Шелухина, так и зарубежных исследователей J. Cannady, H. Debar, A.A. Ghorbani, S.A. Hofmeyr, W. Lu, V. Paxson, M. Tavallaee и др. Анализ работ в этой области показал, что для обнаружения сетевых атак отсутствует гибкая методика обучения коллектива адаптивных бинарных классификаторов, и большинство

исследований ограничивается рассмотрением только одной схемы комбинирования решателей. Поэтому диссертационное исследование направлено на разработку обобщенного подхода к построению универсальной структуры для хранения и представления классификаторов — дерева классификаторов и алгоритма каскадного обучения его узлов, что позволит в контексте выявления аномальных сетевых соединений объединять разнородные решатели без строгой привязки к агрегирующей их выходы композиции и повысить эффективность СОА за счет возможности выбора наилучшей схемы комбинирования решателей.

Научная задача — разработка модельно-методического аппарата для обнаружения аномальных сетевых соединений на основе гибридизации методов ВИ.

Объектом исследования являются распределенные сетевые атаки, механизмы их обнаружения и распределенные СОА.

Предметом исследования являются модели, методики и алгоритмы обнаружения аномальных сетевых соединений на основе ВИ.

Целью диссертационного исследования является повышение эффективности функционирования СОА при помощи оригинального модельно-методического аппарата, основанного на подходе «гибридизация методов ВИ». Для достижения поставленной цели решены следующие **задачи**:

1) анализ сигнатурных и эвристических методов обнаружения сетевых атак;

2) разработка программных инструментов для тестирования сетевых СОА и оценка их возможностей;

3) разработка модели искусственной иммунной системы на базе эволюционного подхода для классификации сетевых соединений;

4) разработка алгоритма генетико-конкурентного обучения сети Кохонена для обнаружения аномальных сетевых соединений;

5) разработка методики иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений;

6) разработка архитектуры и программная реализация распределенной СОА, построенной на основе гибридизации методов ВИ и сигнатурного анализа;

7) разработка программного стенда для генерации сетевых атак и экспериментальная оценка разработанной СОА.

Научная новизна диссертационного исследования заключается в следующем:

1) 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;

2) 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;

3) разработанная методика иерархической гибридизации бинарных классификаторов (детекторов) для обнаружения аномальных сетевых соединений отличается от известных возможностью задания произвольной вложенности клас-

сификаторов друг в друга и их «ленивым» подключением благодаря наличию алгоритма каскадного обучения узлов, осуществляющего эффективный нисходящий спуск по всем цепочкам зависимостей корневого классификатора. Особенность методики заключается в возможности гибкого объединения детекторов для построения единого верхнеуровневого классификатора при помощи различных низкоуровневых схем их комбинирования и агрегирующих композиций.

4) разработанная архитектура распределенной СОА, построенной на основе гибридизации методов ВИ и сигнатурного анализа, отличается от известных возможностью «горячей» вставки (или замены старого) исполняемого кода, содержащего функционирование классификатора, без останова системы («на лету»), наличием интерпретатора для написания собственных сценариев, задающих структуры и правила обучения классификаторов, а также поддержкой оригинальной методики иерархической гибридизации детекторов. В отличие от других программных решений, данная СОА обладает существенно более высокой скоростью обработки сетевых потоков и более низким ресурсопотреблением.

Теоретическая и практическая значимость. Разработанные компоненты предназначены для повышения корректности детектирования сетевых атак, что позволит обеспечить необходимый уровень защищенности информационных ресурсов. Использование разработанной методики гибридизации бинарных классификаторов предоставит возможность объединить разнородные средства обнаружения сетевых атак (включая сигнатурный анализ и различные адаптивные методы) для создания гибридной СОА. За счет использования детекторов в качестве минимальной единицы классификации сетевых атак проектирование СОА ведется в стиле «снизу-вверх»: вначале ее ядро приспосабливается под выявление индивидуальных типов атак, затем оно строит правила (комбинирует детекторы, разрешает конфликты, формирует входные сигналы для классификаторов, выполняет обход дерева классификаторов) для соотнесения подозрительного 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.

Методология и методы диссертационного исследования заключаются в постановке и формализации задач, связанных с обнаружением аномальных сетевых соединений, и включают методы теории множеств, теории ВИ, теории формальных языков, теории вероятностей, теории защиты информации.

Положениями, выносимыми на защиту, являются:

1) модель искусственной иммунной системы на базе эволюционного подхода для классификации сетевых соединений;

2) алгоритм генетико-конкурентного обучения сети Кохонена для обнаружения аномальных сетевых соединений;

3) методика иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений;

4) архитектура и программная реализация распределенной СОА, построенной на основе гибридизации методов ВИ и сигнатурного анализа.

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 результатами, полученными при проведении экспериментов, а также публикацией в ведущих рецензируемых изданиях российского и международного уровня.

Реализация результатов работы. Представленные в диссертационной работе исследования использовались в рамках следующих научно-исследовательских работ: (1) Гранта Российского научного фонда „Управление инцидентами и противодействие целевым кибер-физическим атакам в распределенных крупномасштаб-

ных критически важных системах с учетом облачных сервисов и сетей Интернета вещей“, № 15-11-30029, 2015–2017; (2) Проекта Минобрнауки России „Разработка технологий интерактивной визуализации неформализованных данных разнородной структуры для использования в системах поддержки принятия решений при мониторинге и управлении информационной безопасностью информационно-телекоммуникационных систем“, № 14.604.21.0137, 2014–2016; (3) Проекта Минобрнауки России „Перспективные методы корреляции информации безопасности и управления инцидентами в критически важных инфраструктурах на основе конвергенции технологий обеспечения безопасности на физическом и логическом уровнях“, № 14.616.21.0028, 2014–2014. Полученные результаты внедрены в учебный процесс подготовки магистров по курсу „Advanced Network & Cloud Security“ (проект ENGENSEC TEMPUS № 544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR), используются в учебном процессе Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича и Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики.

Апробация результатов работы. Основные результаты диссертационного исследования были представлены на ряде международных и российских конференций, в том числе: 18-я IEEE международная конференция Computational Science and Engineering (Порто, Португалия, 2015), 7-я международная конференция Mathematical Methods, Models and Architectures for Computer Networks Security (Варшава, Польша, 2017), „Информационные технологии в управлении“ (Санкт-Петербург, 2012 г., 2016 г.), „Информационная безопасность регионов России“ (Санкт-Петербург, 2015 г., 2017 г.), „РусКрипто“ (Московская область, г. Солнечногорск, 2015 г., 2018 г.), „Региональная информатика“ (Санкт-Петербург, 2016 г.), „Актуальные проблемы инфокоммуникаций в науке и образовании“ (Санкт-Петербург, 2018 г.) и др.

Личный вклад. Все результаты, представленные в диссертационной работе, получены лично автором в процессе выполнения научно-исследовательской деятельности.

Публикации. Основные результаты, полученные в ходе диссертационного исследования, изложены в 21 печатном издании, шесть из которых опубликованы в журналах, рекомендованных ВАК, три — в зарубежных изданиях, индексированных в Web of Science и Scopus, 12 — в прочих изданиях. Получено три свидетельства о государственной регистрации программ для ЭВМ.

Структура и объем диссертационной работы. Диссертация состоит из введения, трех глав, заключения и пяти приложений. Основной материал изложен на 204 страницах. Полный объем диссертации составляет 305 страниц с 80 рисунками и 25 таблицами. Список литературы содержит 213 наименований.

Содержание работы

Во **введении** обоснованы актуальность и важность затронутой в диссертационной работе темы исследований, определена цель и сформулированы задачи, решение которых необходимо выполнить для ее достижения. Показаны научная новизна и практическая значимость работы. Представлено краткое описание выносимых на защиту результатов: модели, алгоритма, методики и архитектуры СОА для обнаружения аномальных сетевых соединений с применением методов ВИ.

Первая глава посвящена анализу проблемы обнаружения аномальных сетевых соединений. Выполнен анализ методов обнаружения сетевых атак, предложена их классификация. Определены место и роль методов ВИ в областях искусственного интеллекта и обнаружения аномальных сетевых соединений. Представлены примеры использования конечных автоматов совместно с эволюционными

вычислениями (генетическими алгоритмами и генетическим программированием) для решения данной задачи, предложен ряд рекомендаций по применению методов ВИ в рамках решаемой задачи. Приведена классификация СОА, и представлена общая архитектура сетевой распределенной СОА. Сформулирован список требований, предъявляемых к СОА. Выполнена постановка задачи исследования, которая заключается в разработке модельно-методического аппарата для обнаружения аномальных сетевых соединений на основе гибридизации методов ВИ. Сформулирована цель исследования — повышение эффективности функционирования СОА через снижение значения функционала эмпирического риска на объектах контрольной выборки.

Во **второй главе** представлены разработанные модель искусственной иммунной системы на базе эволюционного подхода, алгоритм генетико-конкурентного обучения сети Кохонена и методика иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений.

Разработанная *модель* искусственной иммунной системы на базе эволюционного подхода представляется следующим образом:

$$AISEA = \langle \mathcal{D}_\mathcal{T}, \mathcal{D}_\mathcal{M}, \mathcal{S}_\mathcal{A}, \mathcal{S}_\mathcal{N}, \mathcal{G}, R, \Psi \rangle, \tag{1}$$

где $\mathcal{D} = \mathcal{D}_\mathcal{T} \bigcup \mathcal{D}_\mathcal{M}$ — набор иммунных детекторов, $\mathcal{D}_\mathcal{T} \subset \mathcal{D}$ — набор временных иммунных детекторов, $\mathcal{D}_\mathcal{M} \subset \mathcal{D}$ — набор иммунных детекторов памяти, $\mathcal{S}$ — набор всевозможных входных объектов, $\mathcal{S}_\mathcal{A} \subset \mathcal{S}$ — обучающий набор, состоящий из аномальных экземпляров („чужих“ объектов), $\mathcal{S}_\mathcal{N} \subset \mathcal{S}$ — тестирующее множество, состоящее из нормальных экземпляров („своих“ объектов), $\mathcal{G} = \{G_1, \ldots, G_K\}$ — стратегии генетической оптимизации иммунных детекторов, $R : \mathcal{D} \times 2^{\mathcal{S}_\mathcal{A}} \times 2^{\mathcal{S}_\mathcal{N}} \times \mathcal{G} \to \mathcal{D}$ — правило обучения иммунных детекторов, $\Psi : \mathcal{D} \times \mathcal{S} \to \mathbb{R}_+$ — функция вычисления аффинности (правило соответствия) между иммунным детектором $d \in \mathcal{D}$ и тестовым объектом $s \in \mathcal{S}$.

Каждый иммунный детектор $d \in \mathcal{D}$ представляется как кортеж следующего вида:

$$d = \langle representation, threshold, life\_time, state \rangle, \tag{2}$$

где $representation \in \{BitString, RealVector, NeuralNetwork, PetriNet, \ldots\}$ — внутреннее представление (внутренняя структура) иммунного детектора d, который может быть задан как двоичная строка с правилом r-непрерывных битов ($BitString$), вещественнозначный вектор ($RealVector$), нейронная сеть ($NeuralNetwork$), сеть Петри ($PetriNet$) и т.д., $threshold \in \mathbb{R}_+$ — порог активации иммунного детектора d, $life\_time \in \mathbb{R}_+^*$ — срок жизни иммунного детектора d, $state \in \{immature, semimature, mature, memory\}$ — текущее состояние иммунного детектора d, которое может представлять собой незрелое, полузрелое, зрелое состояние или состояние, соответствующее детектору памяти. Здесь $\mathbb{R}_+ = [0, +\infty)$, $\mathbb{R}_+^* = \mathbb{R}_+ \bigcup \{+\infty\}$.

Разработанная модель искусственной иммунной системы (формулы 1, 2) — это набор иммунных детекторов, представленных в виде временных детекторов и детекторов памяти, в совокупности с заданным алгоритмом их обучения, который принимает в качестве входных аргументов настраиваемый детектор d, подмножества двух наборов данных (набора $\mathcal{S}_\mathcal{A}$, состоящего из „чужих“ объектов, и набора $\mathcal{S}_\mathcal{N}$, состоящего из „своих“ объектов), а также стратегию генетической оптимизации. Причем набор данных $\mathcal{S}_\mathcal{A}$ предназначается для первой предварительной настройки иммунных детекторов, а роль набора данных $\mathcal{S}_\mathcal{N}$ заключается в фильтрации обученных детекторов. Стратегии генетической оптимизации иммунных детекторов включают некоторый набор генетических операторов (кроссовера, мутации, инверсии и пр.) и их комбинаций для изменения параметров

иммунного детектора после его клонирования. Правило обучения иммунных детекторов представляет собой двухэтапную процедуру. На первом этапе иммунные детекторы обучаются исключительно на элементах набора данных $\mathcal{S}_{\mathcal{A}}$ и подвергаются клональной селекции, в процессе которой созданные копии иммунных детекторов мутируют согласно выбранной стратегии $G' \in \mathcal{G}$. Из набора детекторов, представленного произведенным потомством и исходным детектором, отбираются только те детекторы, которые являются наиболее пригодными по отношению к элементам набора $\mathcal{S}_{\mathcal{A}}$ согласно выбранному правилу соответствия Ψ. Данный этап повторяется несколько раз для формирования полузрелых детекторов. На втором этапе обучения эти детекторы проверяются на соответствие „своим“ объектам: переобучению подвергаются только те детекторы, которые ложно активируются. В рамках данной модели каждый иммунный детектор подвергается нескольким этапам дифференцировки. На рисунке 1 представлены процессы жизненного цикла иммунного детектора вместе с указанными этапами его дифференцировки.

Рисунок 1 — Жизненный цикл иммунного детектора

В процессе функционирования СОА временные детекторы осуществляют запись параметров атак в обновляемый набор аномальных данных $\mathcal{S}_{\mathcal{A}^*}$ в случае их обнаружения. Все иммунные детекторы, кроме детекторов памяти, наделены конечным сроком жизни. Если в течение данного им срока жизни они не выявили ни одной атаки, они подвергаются повторному обучению на расширенном наборе данных, содержащем элементы $\mathcal{S}_{\mathcal{A}}$ и $\mathcal{S}_{\mathcal{A}^*}$. В то же время если иммунный детектор распознал соединение как аномальное, его срок жизни увеличивается. В отличие от них, детекторы памяти обладают бесконечным сроком жизни и не принимают участия в наполнении обновляемого набора аномальных данных. Для обнаружения каждого класса атаки $c \in \mathcal{C}$ выделяется несколько иммунных детекторов, объединяющихся в класс детекторов $\mathcal{D}_c$ и использующих бутстреп-обучение на разных случайных подвыборках множеств $\mathcal{S}_{\mathcal{A}}$ и $\mathcal{S}_{\mathcal{N}}$.

Набор иммунных детекторов памяти определяется следующим образом:

$$\mathcal{D}_{\mathcal{M}} = \bigcup_{c \in \mathcal{C}} \left\{ \operatorname{Arg}\max_{d \in \mathcal{D}_c} \left(\sum_{s \in \mathcal{S}_{\mathcal{A}}^{(d)} \bigcap c} \Psi(d,s) \Big/ \# \left(\mathcal{S}_{\mathcal{A}}^{(d)} \bigcap c \right) \right) \right\}. \tag{3}$$

Порог активации иммунного детектора $d \in \mathcal{D}$, обученного на наборах $\mathcal{S}_{\mathcal{A}}^{(d)} \subseteq \mathcal{S}_{\mathcal{A}}$ и $\mathcal{S}_{\mathcal{N}}^{(d)} \subseteq \mathcal{S}_{\mathcal{N}}$, вычисляется следующим образом:

$$threshold = \frac{h_d^- + h_d^+}{2} = \frac{\min\limits_{s \in \mathcal{S}_{\mathcal{A}}^{(d)}} \Psi(d,s) + \max\limits_{s \in \mathcal{S}_{\mathcal{N}}^{(d)}} \Psi(d,s)}{2}. \tag{4}$$

Формула 4 применяется для вычисления порога активации только тех детекторов d, которые после обучения на множестве аномальных данных $\mathcal{S}_{\mathcal{A}}^{(d)}$ не имеют ложных срабатываний на множестве нормальных данных $\mathcal{S}_{\mathcal{N}}^{(d)}$, т.е. $\forall s' \in \mathcal{S}_{\mathcal{N}}^{(d)}\ \Psi(d,s') < h_d^-$. При выполнении этого условия возникает возможность „сдвинуть“ граничное значение h_d^-, обеспечивающее реагирование детектора d на любой „чужой“ объект $s \in \mathcal{S}_{\mathcal{A}}^{(d)}$, на величину $\frac{h_d^- - h_d^+}{2}$ в сторону h_d^+: $threshold = h_d^- - \frac{h_d^- - h_d^+}{2} = \frac{h_d^- + h_d^+}{2}$.

Классификация объекта $s \in \mathcal{S}$ при помощи рассмотренной модели искусственной иммунной системы представлена в алгоритме 1.

Алгоритм 1: Классификация сетевых соединений с помощью $AISEA$

---

1. Вычисление для каждого иммунного детектора $d \in \mathcal{D}$ значения его активации $a_d = \Psi(d,s) - threshold$. Считается, что, если $a_d \geqslant 0$, то детектор d является активировавшимся, в противном случае соответствующий детектор не реагирует на входной объект s.
2. Мажоритарное голосование внутри каждого класса детекторов $\mathcal{D}_c$. Если $\left(A_c \leftrightharpoons \sum\limits_{d \in \mathcal{D}_c} [a_d \geqslant 0]\right) > \left(B_c \leftrightharpoons \sum\limits_{d \in \mathcal{D}_c} [a_d < 0]\right)$, то s распознается как „чужой“ объект. Если $A_c < B_c$, то s распознается как „свой“ объект. В случае наличия конфликтов, т.е. $A_c = B_c$, s классифицируется как „чужой“ объект, если $a_{d_m^{(c)}} \geqslant 0$, и s классифицируется как „свой“ объект, если $a_{d_m^{(c)}} < 0$, где $d_m^{(c)} \in \mathcal{D}_{\mathcal{M}} \bigcap \mathcal{D}_c$, т.е. $d_m^{(c)}$ — детектор памяти, обученный для распознавания „своего“ объекта и „чужого“ объекта из класса c.
3. Формирование множества классов активировавшихся иммунных детекторов $\{\mathcal{D}_{c'}\}_{c' \in \mathcal{C}^*}$, которые распознают входной объект s как „чужой“ объект, где $\mathcal{C}^* = \left\{ c' \,\middle|\, (c' \in \mathcal{C}) \wedge \left((A_{c'} > B_{c'}) \vee \left((A_{c'} = B_{c'}) \wedge (a_{d_m^{(c')}} \geqslant 0) \right) \right) \right\} \subset \mathcal{C}$.
4. Определение класса объекта s. Если $\mathcal{C}^* = \varnothing$, то объект s относится к классу „своих“ объектов. Если $E_{\mathcal{C}^*} \leftrightharpoons \max\limits_{c' \in \mathcal{C}^*} A_{c'}$ достигается в одной единственной точке, то класс объекта s — это $\arg E_{\mathcal{C}^*}$, иначе класс объекта s — это $\arg \max\limits_{c' \in \{\arg E_{\mathcal{C}^*}\}} \sum\limits_{d \in \mathcal{D}_{c'}} a_d \cdot [a_d \geqslant 0]$.

Данный алгоритм основан на сравнении величины аффинности иммунных детекторов с их индивидуально настроенными порогами активации и учете одинаковых голосов, полученных от большей части детекторов. В случае возникновения конфликтов при различении между нормальным и аномальным классом (шаг 2) решающий голос отдается детектору памяти. Если же после этого сохраняется конфликт на уровне группы детекторов, то принимается во внимание сумма величин аффинности именно активировавшихся в ответ на данный стимул (входной объект) иммунных детекторов (шаг 4). Входной объект является „своим“ тогда и только тогда, когда $\forall c \in \mathcal{C}\ \ (A_c < B_c) \vee \left((A_c = B_c) \wedge (a_{d_m^{(c)}} < 0) \right)$. В качестве основы для данной модели (M_3) использовались модель с жизненным циклом (M_1), предложенная Hofmeyr и Forrest, и модель с библиотекой генов (M_2), предложенная Kim и Bentley. Сравнение этих трех моделей приведено в таблице 1. Знаком „+“ отмечены те характеристики, которые присущи соответствующей модели, знак „−“ означает отсутствие поддержки этой особенности у модели.

Таблица 1 — Сравнение иммунных моделей для обнаружения сетевых атак

Иммунная модель	Сравниваемые характеристики											
	Независимость от внутренней структуры иммунного детектора	Наличие клональной селекции и генетической оптимизации	Наличие отрицательного отбора	Автоматический подбор порога активации иммунного детектора	Наличие двухступенчатого алгоритма обучения иммунных детекторов	Наличие детекторов памяти	Наличие жизненного цикла лимфоцитов	Динамическое переобучение	Обучение детекторов на новых данных в процессе функционирования системы	Распределенность иммунных детекторов (передача их на другие сетевые узлы)	Поддержка мультиклассового обнаружения сетевых атак	Автономность иммунной системы (функционирование без привлечения оператора)
M_1	−	−	+	−	−	+	+	+	+	−	−	−
M_2	−	+	+	−	−	+	−	+	+	+	−	+
M_3	+	+	+	+	+	+	+	+	+	−	+	+

В качестве внутреннего представления иммунных детекторов были выбраны карты Кохонена, для которых был разработан *алгоритм* генетико-конкурентного обучения. Оптимизация направлена на сокращение числа эпох обучения посредством корректировки весов «мертвых» нейронов. Для имитации процесса эволюции нейронов было разработано несколько способов генерации порождаемых ими поколений. Первый подход A_1 заключается в применении операторов скрещивания, мутации или инверсии произвольных нейронов, находящихся в текущей близости от нейрона-победителя. Второй подход A_2 основан на геометрических соображениях о взаимном расположении нейронов на выходной решетке относительно нейрона-победителя: поскольку весовой вектор каждого нейрона, равноотстоящего от нейрона-победителя, модифицируется с одинаковым коэффициентом в результате выполнения выбранного алгоритма обучения, то и оператор скрещивания предлагается применять именно к таким нейронам. Третий подход A_3 подразумевает применение оператора скрещивания только к наиболее приспособленным особям, в то время как к оставшимся нейронам будет применяться оператор мутации или инверсии. Здесь в роли функции приспособленности было выбрано обратное значение величины среднего отклонения при распознавании данным нейроном с весовым коэффициентом $\boldsymbol{w_{ij}}$ элементов обучающей выборки $\{\boldsymbol{x_k}\}_{k=1}^{M}$: $\Psi_{ij} = \left(\frac{\sum_{k=1}^{M}\|\boldsymbol{x_k}-\boldsymbol{w_{ij}}\|}{M}\right)^{-1}$ для пакетного обучения либо $\Psi_{ijk} = \|\boldsymbol{x_k} - \boldsymbol{w_{ij}}\|^{-1}$ для интерактивного обучения. Кроме того, было разработано несколько стратегий для выбора того или иного способа генерации нейронов: фиксированный выбор определенного подхода G_1, последовательный или случайный перебор всех подходов G_2 и выбор, основанный на механизме рулетки G_3. В стратегии G_3, если сгенерированное при помощи выбранного подхода потомство нейронов является более приспособленным по сравнению с предками, то вероятность выбора такого подхода в будущем увеличивается по сравнению с остальными подходами, иначе вероятность его выбора уменьшается. Каждая из стратегий G_1, G_2, G_3 манипулирует выбором одного из подходов A_1, A_2, A_3. Отметим, что помимо конкуренции между нейронами (согласно алгоритму конкурентного обучения сети Кохонена) в случае стратегии G_3 создается также конкурентная борьба между подходами за право генерировать дочерние поколения нейронов.

Разработанная *методика* иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений показана на рисунке 2 и состоит из следующих этапов: (1) построение дерева классификаторов; (2) формирование параметров сетевых соединений; (3) предобработка параметров сетевых соединений; (4) иерархический обход дерева классификаторов в ширину; (5) обнаружение аномальных сетевых соединений.

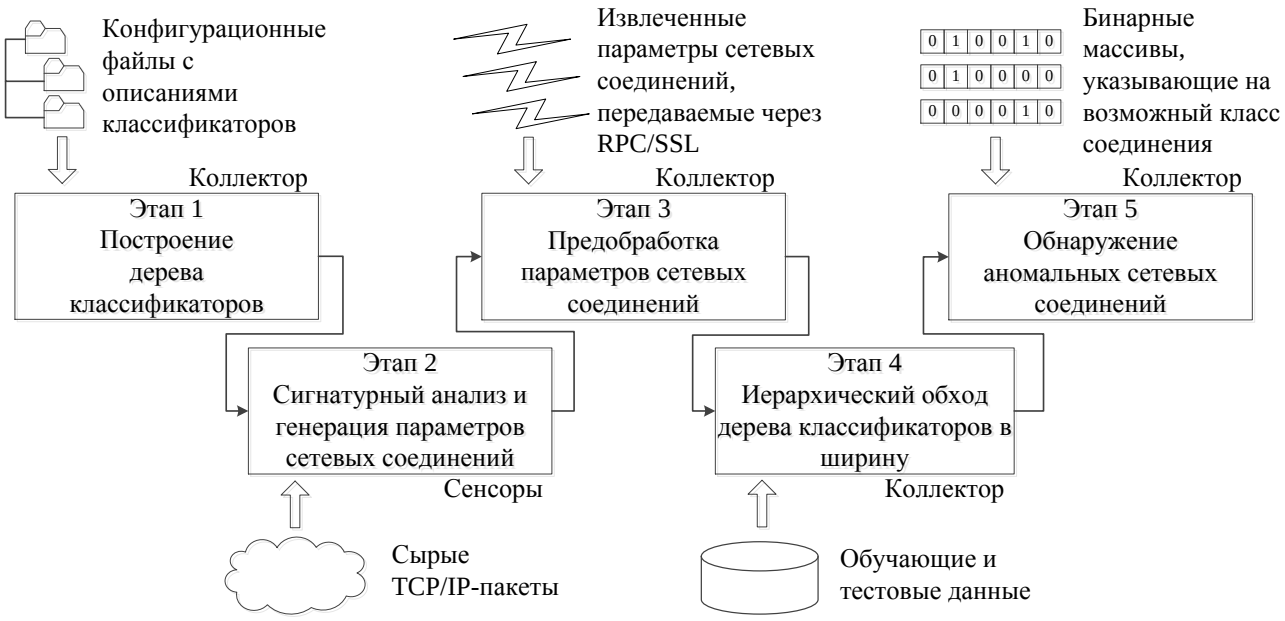

Рисунок 2 — Этапы методики иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений

Первый этап методики является подготовительным, он заключается в выборе структуры отдельных бинарных классификаторов (детекторов): размерности и числа слоев, параметров и алгоритмов обучения, типов функций активации, функций принадлежности и ядерных функций. Для каждого детектора может быть составлен набор обучающих правил, который позволит объединить группу детекторов в классификатор на на основе подходов «один-ко-всем» (one-vs-all), «один-к-одному» (one-vs-one) или их различных производных вариаций (классификационное бинарное дерево, направленный ациклический граф). Для построения коллективного правила (агрегирующей композиции) G, объединяющего выходные результаты классификаторов $F^{(i)}$, были реализованы следующие подходы: (1) метод мажоритарного голосования (ММГ), или метод голосования большинством; (2) метод взвешенного голосования (МВГ), приписывающий классификаторам весовые коэффициенты; (3) метод многоярусной укладки (ММУ), дополненный введением атрибута — номера кластера по методу K-средних; (4) метод Фикса—Ходжеса (МФХ), представляющий собой объединение классификаторов с использованием арбитра на основе динамических областей компетентности и метода ближайших соседей. Данная методика подразумевает распределенную архитектуру реализующих ее систем, в которых сбор данных осуществляется вторичными узлами — сенсорами, а вся обработка агрегированных потоков данных выполняется на централизованном сервере — коллекторе.

Второй этап методики, выполняемый на стороне сенсоров, заключается в применении разработанного алгоритма сборки сырых пакетов в сетевые соединения, выделении их параметров и выполнении сигнатурного анализа с использованием нескольких разработанных параллельных модификаций алгоритмов шаблонного поиска подстроки. С этой целью было исследовано быстродействие алгоритмов Ахо—Корасик и Бойера—Мура на выбранных сигнатурных

записях Snort, и реализованы их улучшенные аналоги при помощи технологий OpenMP и CUDA. Был реализован событийно-ориентированный анализатор сетевого трафика, с помощью которого было извлечено 106 сетевых параметров. Для измерения величины интенсивности отправки/приема пакетов использовался адаптированный метод скользящей средней.

Третий этап методики начинается с прослушивания входящих от сенсоров пакетов, передаваемых по протоколу RPC/SSL и содержащих вычисленные параметры соединений. Перед непосредственным обучением детекторов выполняется предобработка данных параметров (нормализация) для уменьшения эффекта их сильной изменчивости. Далее выполняется уменьшение числа значимых признаков, которое достигается при помощи метода главных компонент. Результаты экспериментов показали, что повторная нормализация после сжатия при помощи метода главных компонент необязательна.

Четвертый этап методики с точки зрения вычислительных ресурсов является наиболее трудоемким и состоит из следующих рекурсивно повторяющихся последовательностей действий: вычисление зависимостей текущего классификатора, формирование входных сигналов для текущего классификатора, обучение текущего классификатора (алгоритм 2). Была разработана специальная древовидная структура для хранения классификаторов, которая позволяет осуществлять эффективный нисходящий спуск по всем цепочкам зависимостей, начиная с верхнеуровневого классификатора до терминальных узлов, представленных детекторами. Следствием используемого таким образом каскадного обучения является возможность «ленивой» загрузки классификаторов. Это свойство является особенно выгодным при разборе динамических правил обучения классификаторов, т.е. таких правил, от успешного или неуспешного срабатывания которых зависит вызов другого правила. В частности, это характерно для классификационного дерева, когда правила являются вложенными друг в друга.

Алгоритм 2: Каскадное обучение дерева классификаторов

```
1  функция f_1 конвертирования дерева классификаторов cls_tree в 1-направленный список dir_list
2  начало блока
3      dir_list :=создать пустой список
4      добавить корень root_node дерева cls_tree в качестве головного элемента в список dir_list
5      list_elem :=получить головной элемент списка dir_list (root_node)
6      пока list_elem не равен NULL выполнять
7          если узел list_elem не является терминальным в дереве cls_tree тогда
8              для каждого дочернего узла nested_node элемента list_elem выполнять
9                  добавить узел nested_node в качестве хвостового элемента в список dir_list
10         list_elem :=получить следующий за list_elem элемент из списка dir_list
11     возвратить dir_list
12 функция f_2 каскадного обучения узла node и его зависимостей в дереве классификаторов cls_tree
13 начало блока
14     если узел node помечен как необученный тогда
15         если узел node нетерминальный тогда
16             для каждого узла dep_node из списка зависимостей узла node выполнять
17                 вызвать функцию f_2 для узла dep_node
18         in_data :=сформировать входные векторы для узла node согласно его дереву выражений
19         выполнить обучение классификатора, размещенного в узле node, на данных in_data
20         пометить узел node как обученный
21 функция f_3 обхода дерева классификаторов cls_tree в ширину при помощи списка dir_list
22 начало блока
23     node :=получить головной элемент списка dir_list
24     пока node не равен NULL выполнять
25         вызвать функцию f_2 для узла node
26         node :=получить следующий за node элемент из списка dir_list
27 cls_tree :=вызвать интерпретатор для заданного пользователем конфигурационного файла
28 dir_list :=вызвать функцию f_1 для дерева классификаторов cls_tree
29 вызвать функцию f_3 для дерева классификаторов cls_tree и списка dir_list
```

Пятый этап методики включает два режима: режим оценки эффективности и режим функционирования. В первом режиме осуществляется вычисление показателей оценки качества классификационных моделей, во втором режиме выполняется диагностика системы без априорного знания о фактическом классе идентифицируемого сетевого соединения. Для оценки эффективности СОА, разработанной на основе этой методики, было выбрано восемь показателей: (1) показатель корректности обнаружения сетевых атак (TPR); (2) показатель ложных срабатываний (FPR); (3) показатель корректности классификации соединений (CCR); (4) показатель некорректной классификации (ICR); (5) показатель обобщающей способности при обнаружении (GPR); (6) показатель переобученности при обнаружении (OPR); (7) показатель обобщающей способности при классификации (GCR); (8) показатель переобученности при классификации (OCR).

Третья глава посвящена разработке *архитектуры* и программной реализации сетевой распределенной СОА, а также экспериментальной оценке предложенных модели, алгоритма и методики.

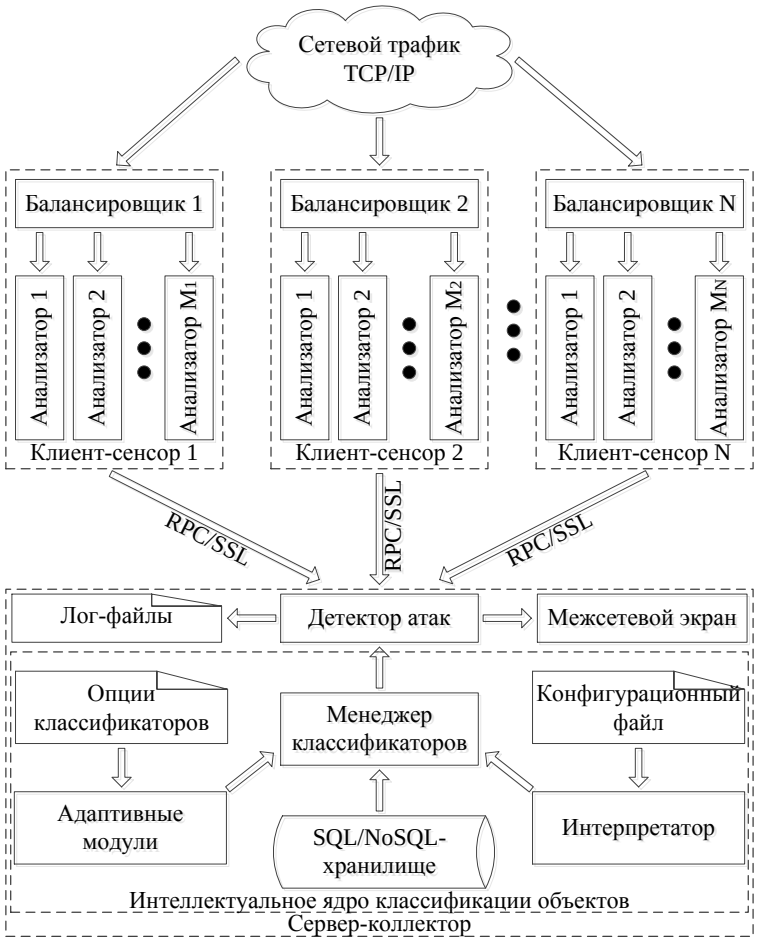

Рисунок 3 — Архитектура разработанной СОА

Разработанная СОА является распределенной и состоит из нескольких клиент-сенсоров и одного сервер-коллектора (рисунок 3). На каждый контролируемый узел в сети устанавливается два программных компонента: балансировщик трафика и сетевой анализатор. Роль первого заключается в распределении нагрузки между несколькими внутренними фиктивными интерфейсами ОС. Функции анализатора — дефрагментация IP-пакетов, формирование TCP-сессий (TCP-реассемблирование), выделение атрибутов сетевого трафика, включая сбор статистических показателей по входящим IP-адресам, измерение интенсивности приема специальных пакетов. Кроме того, в число задач этого компонента добавлено обнаружение явных нарушений на уровне сети (выявление land-атак, аномальных сетевых пакетов и подозрительных исходящих адресов), проверка целостности пакетов посредством вычисления их контрольных сумм, выполнение сигнатурного анализа содержимого отдельных и дефрагментированных пакетов, а также контента реассемблированных TCP-сегментов. Для корректной обработки потока фрагментированных IP-пакетов разработаны алгоритмы, свойственные сетевому стеку ОС Linux. В зависимости от сетевой нагрузки на сенсоре может быть запущено несколько анализаторов, каждый из которых прослушивает сетевой трафик на определенном интерфейсе, являющемся выходным для балансировщика.

Реализовано 20 плагинов, предназначенных для загрузки в интеллектуальное ядро классификации объектов, что позволяет экспериментально исследовать несколько адаптивных детекторов с различными настройками их параметров, алгоритмов их обучения и схем их комбинирования. При разработке плагинов использовалось 5 языков программирования: C, C++, Perl, Python, R.

Исследование адаптивных свойств модели искусственной иммунной системы и алгоритма генетико-конкурентного обучения сети Кохонена осуществлялось при помощи набора данных, содержащего три класса сетевых соединений: сканирование хостов (scan), отказ в обслуживании (synflood) и легитимный трафик (normal). На рисунке 4 показан график ошибки векторного квантования для стандартного и модифицированного алгоритмов обучения сети Кохонена на подвыборке, соответствующей экземплярам класса scan.

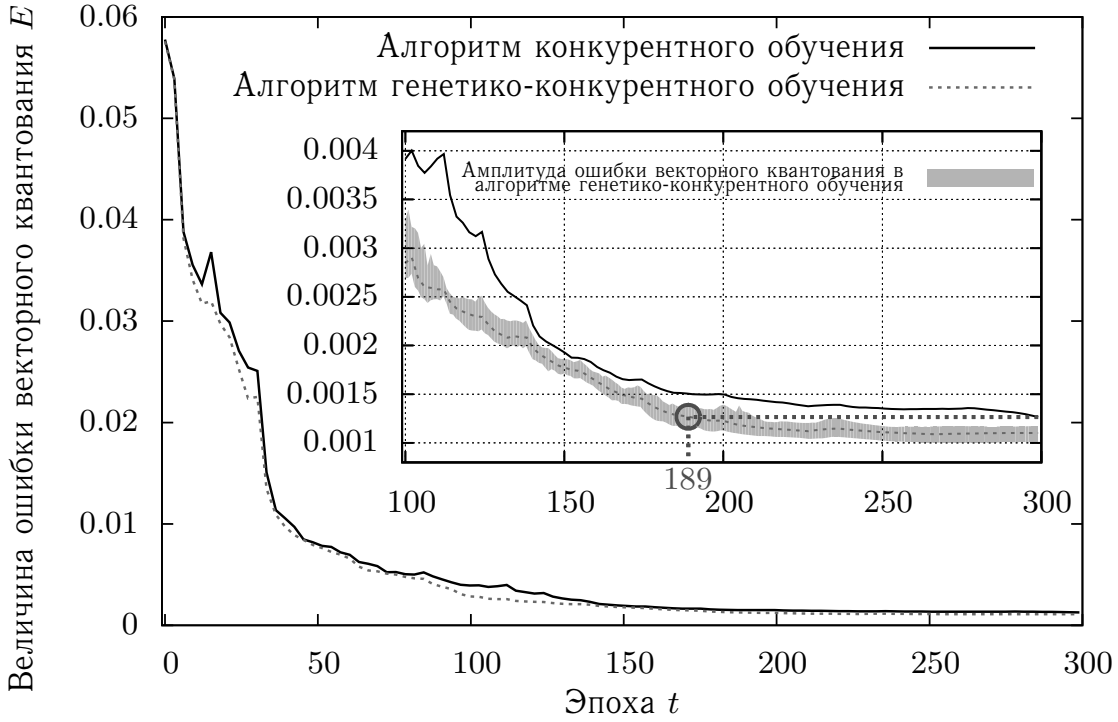

Рисунок 4 — График ошибки векторного квантования для класса scan

Наименьшее значение ошибки векторного квантования, достигаемое стандартным алгоритмом на 299-ой эпохе, выполняется для оптимизированного алгоритма уже после 189-ой эпохи. Введение стратегий генетической оптимизации позволило сократить функционирование алгоритма на 110 эпох.

Выполненные для иммунной системы эксперименты показали, что при помощи корректировки порогов максимум показателя TPR увеличился на 19.5% на контрольном множестве из 7500 элементов и на 47.6% на контрольном множестве из 30000 элементов, при этом максимальное значение показателя ложных срабатываний FPR осталось прежним (2.4%) для первого контрольного множества и поднялось всего лишь на 0.1% для второго контрольного множества (рисунок 5). Наибольшее значение показателя CCR с применением корректировки порогов на контрольном множестве из 7500 и 30000 элементов составило соответственно почти 97.5% и 88.2%, что на 13.1% и 31.4% превышает аналогичный показатель, вычисленный без корректировки порогов на соответствующих множествах данных; вместе с этим максимальное значение показателя ICR опустилось на 6% и 8% соответственно. Данные эксперименты выполнялись 100 раз для вычисления усредненных показателей.

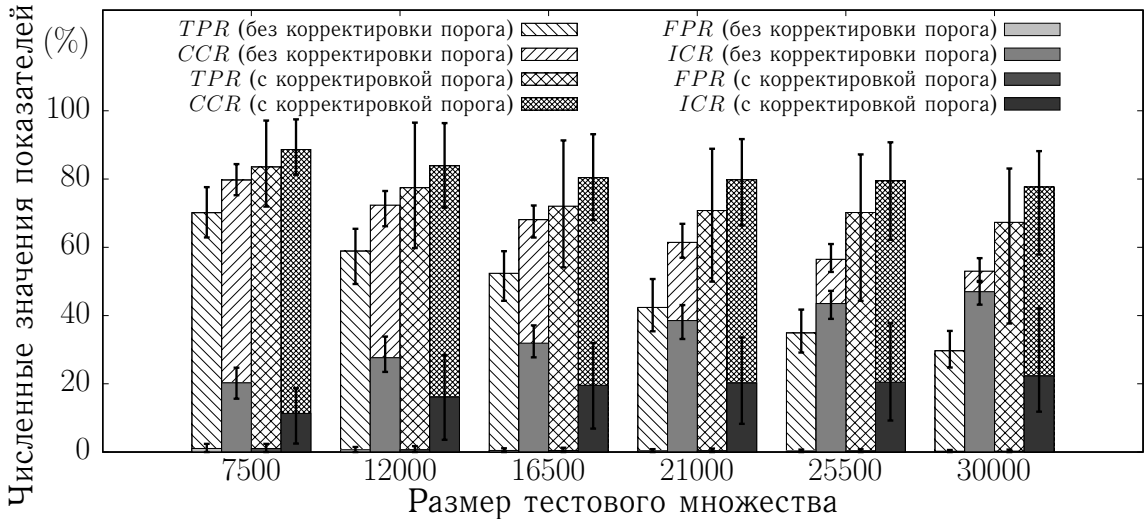

Рисунок 5 — Показатели эффективности для иммунной системы

Для оценки эффективности гибридных подходов использовался открытый набор данных DARPA 1998. В качестве базовых классификаторов $F^{(i)}$ были выбраны машины опорных векторов (МОВ), нейронечеткие сети типа ANFIS (ННС), многослойные нейронные сети (МНС), нейронные сети с радиальными базисными функциями (РБФ) и рекуррентные нейронные сети Джордана (РНС). Одной из наиболее важных характеристик вычислительно интеллектуальных систем является их обобщающая способность, т.е. корректность классификации уникальных экземпляров контрольной выборки, исключающей любые обучающие объекты. Применение пятиблочной кросс-валидации показало, что показатели $GPR - FPR$ и $GCR - ICR$ для МФХ выросли на 0.142% и 1.275% по сравнению с максимальными значениями этих же показателей, демонстрируемых среди базовых классификаторов (рисунок 6).

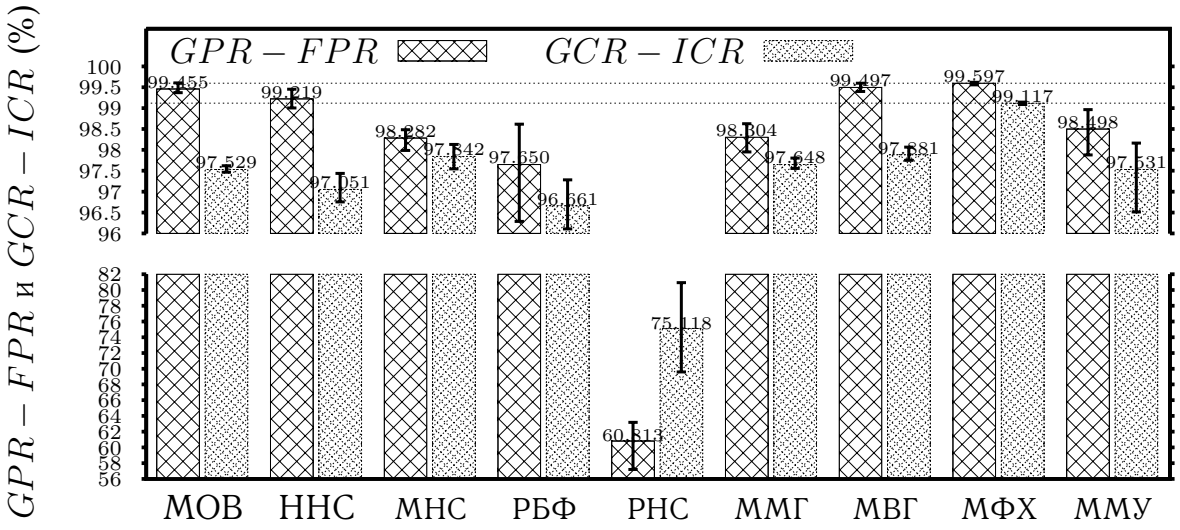

Рисунок 6 — Показатели эффективности для схемы one-vs-all

Введение двух ошибочных классификаторов в коллектив, построенный на основе схемы one-vs-all, показало, что СОА сохраняет устойчивость к наличию шумов. В частности, для МФХ средние значения показателей $GPR - FPR$ и $GCR - ICR$ снизились на несущественные 0.005% и 0.073%.

Характеристики разработанного сетевого сенсора сравнивались с такими СОА, как Snort, Suricata и Bro. Средняя скорость обработки пакетов сенсором составляет 324.756 килопакетов в секунду, что более чем в 1.5 раза превышает этот

же показатель, вычисленный для Suricata в режиме single, при этом размер потребляемой реальной памяти почти в 1.5 раза ниже, чем у указанной СОА.

Результаты выполненных экспериментов доказывают, что разработанная СОА удовлетворяет требованиям, предъявляемым к вычислительно интеллектуальным системам, а именно она (1) является адаптивной в терминах ВИ, (2) обладает способностью обобщения, (3) устойчива к наличию шумов, (4) характеризуется высокой скоростью функционирования.

В **заключении** приведены основные научные результаты диссертационного исследования. В **приложениях** выполнен анализ пяти открытых СОА, произведено их тестирование с целью проверки способности к обнаружению атак со скрытием и со вставкой, приведены примеры обнаружения сетевой атаки типа „подбор пароля“ средствами каждой СОА, представлены грамматика интеллектуального ядра классификации объектов, результаты экспериментов и копии актов о внедрении результатов диссертационной работы.

Основные выводы и результаты

В диссертационной работе решена задача разработки модельно-методического аппарата для обнаружения аномальных сетевых соединений на основе гибридизации методов ВИ. Основные результаты сводятся к следующему:

1. Разработана модель искусственной иммунной системы на базе эволюционного подхода. Модель характеризуется наличием двухуровневой процедуры обучения и тестирования и позволяет учитывать динамическую природу сетевого трафика посредством переобучения иммунных детекторов как с течением времени, так и в ответ на выявленные в сетевом трафике аномалии. Встроенный в модель алгоритм группового обнаружения сетевых атак позволяет снизить число конфликтных случаев их классификации. Результаты проведенных экспериментальных исследований подтвердили отсутствие таких ситуаций.

2. Разработан алгоритм генетико-конкурентного обучения сети Кохонена. Отличительной особенностью алгоритма является наличие процесса имитации эволюции «мертвых» нейронов, который достигается за счет использования нескольких стратегий генетической оптимизации весовых коэффициентов сети Кохонена. Дополненная оптимизация позволяет сократить количество эпох обучения при достижении заданной максимальной величины ошибки векторного квантования. В частности, для случая класса scan число эпох обучения было уменьшено на 110 по сравнению со стандартной реализацией алгоритма.

3. Разработана методика иерархической гибридизации бинарных классификаторов. Методика предоставляет возможность строить многоуровневые схемы с произвольной вложенностью классификаторов друг в друга и их «ленивым» подключением в процессе анализа входного вектора. В случае применения пятиблочной кросс-валидации и низкоуровневой схемы one-vs-all для комбинирования детекторов экспериментально было получено увеличение показателя $GCR - ICR$ на 1.275%. Программная реализация этой методики в виде интеллектуального ядра классификации объектов может быть использована обособленно от СОА при решении общих задач классификации объектов.

4. Разработана архитектура распределенной СОА, построенной на основе гибридизациии методов ВИ и сигнатурного анализа. СОА характеризуется возможностью горячей вставки исполняемого кода за счет загрузки плагинов, представленных в виде бинарных библиотек и встраиваемых динамически в ядро СОА. Ее событийно-ориентированный анализатор предоставляет интерфейс для доступа как к полям отдельных пакетов, так и к параметрам реассемблированных сетевых соединений. Эксперименты показали, что скорость обработки сетевых потоков при помощи разработанной СОА более чем в 1.5 раза превышает аналогичный показатель, демонстрируемый другими решениями.

Представленный модельно-методический аппарат позволяет повысить эффективность функционирования СОА и может быть использован как основа для построения систем классификации объектов.

Рекомендации по применению разработанного модельно-методического аппарата для построения СОА включают применение механизмов распараллеливания для обнаружения сетевых атак, использование машинного кода в качестве основы для СОА, разработку подходов, направленных на оптимизацию доступа к памяти. Перспективы дальнейшей разработки темы заключаются в расширении списка вычисляемых сетевых параметров для учета особенностей, свойственных новым типам аномалий, и совершенствовании предложенной архитектуры СОА с целью ее адаптации под современные классы сетевых атак. Полученные результаты соответствуют п. 13 паспорта специальностей ВАК (технические науки) «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» по специальности 05.13.19.

Список публикаций по теме диссертации

В журналах, рекомендованных ВАК

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.

В зарубежных изданиях, индексированных в Web of Science и Scopus

7. *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.
8. *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.
9. *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.

В прочих изданиях

10. *Тимофеев, А. В.* Исследование и моделирование нейросетевого метода обнаружения и классификации сетевых атак / А. В. Тимофеев, А. А. Браницкий // International Journal Information Technologies & Knowledge. — 2012. — Т. 6, № 3. — С. 257—265.
11. *Браницкий, А. А.* Методы и средства распознавания сетевых атак с помощью нейросетевых и иммуноклеточных технологий / А. А. Браницкий, А. В. Тимофеев // Доклады 9-й международной конференции „Интеллектуализация обработки информации“ (ИОИ-9). 17–21 сентября 2012. Черногория, г. Будва. — М. : Торус Пресс, 2012. — С. 677—681.

12. *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. — Издательство „ВВМ“, Санкт-Петербургский государственный университет, 2012. — С. 335—340.
13. *Браницкий, А. А.* Интеллектуальные методы обнаружения и классификации сетевых атак / А. А. Браницкий, А. В. Тимофеев // Тезисы докладов 10-й международной конференции „Интеллектуализация обработки информации“ (ИОИ-10). 4–11 октября 2014. Греция, о. Крит. — М. : Торус Пресс, 2014. — С. 228—229.
14. *Браницкий, А. А.* Методы комбинирования бинарных классификаторов для задач обнаружения и классификации сетевых атак / А. А. Браницкий, И. В. Котенко // Материалы 24-й научно-технической конференции „Методы и технические средства обеспечения безопасности информации“. 29 июня–2 июля 2015 года. Санкт-Петербург. — Издательство Политехнического университета, 2015. — С. 68.
15. *Браницкий, А. А.* Обнаружение вторжений на основе комплексирования сигнатурных методов и механизмов машинного обучения / А. А. Браницкий // Материалы 24-й научно-технической конференции „Методы и технические средства обеспечения безопасности информации“. 29 июня–2 июля 2015 года. Санкт-Петербург. — Издательство Политехнического университета, 2015. — С. 67.
16. *Браницкий, А. А.* Методы вычислительного интеллекта для обнаружения и классификации аномалий в сетевом трафике / А. А. Браницкий // Материалы IX Санкт-Петербургской межрегиональной конференции „Информационная безопасность регионов России“ (ИБРР-2015). 28–30 октября 2015 г. — СПб. : СПОИСУ, 2015. — С. 61—62.
17. *Браницкий, А. А.* Искусственные иммунные системы как концепция обнаружения и классификации атак в условиях динамически изменяющегося трафика / А. А. Браницкий // Материалы 25-й научно-технической конференции „Методы и технические средства обеспечения безопасности информации“. 4–7 июля 2016 года. Санкт-Петербург. — Издательство Политехнического университета, 2016. — С. 12—13.
18. *Браницкий, А. А.* Комбинированный подход к обнаружению сетевых атак на основе сигнатурного анализа и методов вычислительного интеллекта / А. А. Браницкий // Материалы XV Санкт-Петербургской международной конференции „Региональная информатика“ (РИ-2016). 26–28 октября 2016 г. — СПб. : СПОИСУ, 2016. — С. 150.
19. *Браницкий, А. А.* Архитектура распределенной системы обнаружения, классификации и предотвращения сетевых атак на основе сигнатурного анализа и методов вычислительного интеллекта / А. А. Браницкий // Материалы 9-й конференции „Информационные технологии в управлении“ (ИТУ-2016). 4–6 октября 2016 г. — СПб. : АО «ЦНИИ „Электроприбор“», 2016. — С. 651—655.
20. *Браницкий, А. А.* Модифицированная модель вычислительной иммунной системы на базе эволюционно-генетического подхода для обнаружения и классификации аномальных сетевых соединений / А. А. Браницкий // Материалы 9-й конференции „Информационные технологии в управлении“ (ИТУ-2016). 4–6 октября 2016 г. — СПб. : АО «ЦНИИ „Электроприбор“», 2016. — С. 656—659.
21. *Браницкий, А. А.* Методики комбинирования бинарных классификаторов для выявления аномальных сетевых соединений / А. А. Браницкий, И. В. Котенко // Материалы 9-й конференции „Информационные технологии в управлении“ (ИТУ-2016). 4–6 октября 2016 г. — СПб. : АО «ЦНИИ „Электроприбор“», 2016. — С. 660—664.

Свидетельства о государственной регистрации программ для ЭВМ

22. *Браницкий, А. А.* Адаптивная система обнаружения атак на основе гибридизации методов вычислительного интеллекта / А. А. Браницкий, И. В. Котенко. — Свидетельство о государственной регистрации программы для ЭВМ № 2015662189. Зарегистрировано в Реестре программ для ЭВМ 18.11.2015.
23. *Браницкий, А. А.* Компонент классификации аномальных сетевых соединений на основе искусственных иммунных систем / А. А. Браницкий, И. В. Котенко. — Свидетельство о государственной регистрации программы для ЭВМ № 2016663476. Зарегистрировано в Реестре программ для ЭВМ 08.12.2016.
24. *Браницкий, А. А.* Frontend-интерфейс генератора сетевых атак / А. А. Браницкий, И. В. Котенко, И. Б. Саенко. — Свидетельство о государственной регистрации программы для ЭВМ № 2017660184. Зарегистрировано в Реестре программ для ЭВМ 19.09.2017.