Секция «10.5 Компьютерное право и информационная безопасность»

Анализ совместимости с отечественными и зарубежными платформами систем обнаружения вторжений при внедрении адаптивных самоорганизующихся карт с динамической топологией для повышения эффективности выявления малозаметных атак

Научный руководитель – Штеренберг Станислав Игоревич

Зуев Дмитрий Павлович
Студент (магистр)
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия
E-mail: dmitriy.molodec88@gmail.com

Современный ландшафт киберугроз характеризуется ростом малозаметных атак прикладного уровня, включая низкоинтенсивные распределённые атаки типа «отказ в обслуживании», способные имитировать легитимное поведение пользователей за счёт фрагментированных запросов с периодичностью, не превышающей таймауты соединений [3]. Традиционные системы обнаружения вторжений демонстрируют ограниченную эффективность против подобных угроз, что обусловливает необходимость внедрения адаптивных механизмов анализа на основе самоорганизующихся карт с динамической топологией. Критически важным аспектом практического применения таких решений становится их совместимость с гетерогенной инфраструктурой
отечественного производства.

Анализ современных платформ обнаружения вторжений выделяет четыре основных класса систем, каждый из которых обладает специфическими требованиями к интеграции адаптивных нейросетевых модулей [1]. Сигнатурные системы, представленные решениями Snort, Suricata и Zeek, функционируют на основе сопоставления трафика с базой известных шаблонов атак. Их архитектура предусматривает подключение внешних препроцессоров и модулей анализа через стандартизированные интерфейсы, что теоретически позволяет интегрировать самоорганизующиеся карты Кохонена в качестве дополнительного слоя предварительной фильтрации. Однако практическая реализация сталкивается с ограничениями производительности. Сигнатурные системы оптимизированы для высокоскоростной обработки пакетов с минимальной задержкой, тогда как обучение и адаптация карты в реальном времени требует значительных вычислительных ресурсов, что может нарушить баланс между скоростью анализа и глубиной проверки.

Системы обнаружения аномалий, такие как решения от Darktrace, McAfee Network Security Platform и Splunk Enterprise Security, изначально построены на принципах машинного обучения и анализа отклонений от профиля нормального поведения. Их архитектура наиболее благоприятна для внедрения адаптивных карт Кохонена, поскольку уже включает механизмы кластеризации и построения профилей трафика. Ключевым преимуществом интеграции карт с динамической топологией в такие системы становится возможность автоматической адаптации размерности пространства признаков под меняющиеся характеристики сетевой среды. Например, при обнаружении признаков низкоинтенсивной атаки система может временно увеличивать разрешение карты для детального анализа паттернов фрагментации запросов, а в штатном режиме использовать упрощённую топологию для снижения нагрузки на ресурсы. Однако совместимость с отечественными платформами требует разработки специализированных драйверов, обеспечивающих корректную работу нейросетевых вычислений на архитектурах Эльбрус и Байкал без потери производительности.

Гибридные системы, включая Security Onion, Alien Vault USM и Cisco Firepower, объединяют сигнатурный и поведенческий анализ в единой архитектуре. Их модульная структура теоретически позволяет встраивать адаптивные карты Кохонена как независимый компонент анализа аномалий, дополняющий сигнатурный движок. Практическая реализация, однако, осложняется использованием проприетарных форматов данных и закрытых API в коммерческих решениях, таких как Cisco Firepower, что требует разработки специальных адаптеров преобразования данных между внутренними представлениями трафика и входным форматом нейросети. В случае с открытыми платформами вроде Security Onion интеграция оказывается более прозрачной благодаря поддержке стандартных форматов PCAP и унифицированным интерфейсам взаимодействия между компонентами анализа. Особую сложность представляет обеспечение совместимости с отечественными операционными системами Астра Линукс и РЕД ОС, где требуется не только перекомпиляция модулей под альтернативные архитектуры процессоров, но и адаптация под особенности реализации сетевого стека и механизмов межпроцессного взаимодействия.

Четвёртый класс систем специализированные платформы для защиты веб-приложений (WAF). Они демонстрирует наибольший потенциал для внедрения адаптивных карт с динамической топологией [2]. Интеграция карты Кохонена непосредственно в веб-сервер через модули расширения, например NGX JavaScript в NGINX, позволяет анализировать структуру HTTP-запросов в реальном времени по метрикам длины, энтропии, количества специальных символов и паттернов фрагментации. Такая реализация обеспечивает минимальные накладные расходы нагрузка на процессор не превышает 100% одного ядра при потреблении оперативной памяти менее 1%, а скорость обработки достигает 8849 запросов в секунду. Архитектурная независимость подобных решений позволяет их развёртывание как на зарубежных серверных платформах, так и на отечественных решениях, включая серверные сборки на базе процессоров Байкал-М и ОС Астра Линукс. Динамическая топология карты, способная изменять размерность сетки 20 на 20 в зависимости от интенсивности трафика и выявленных аномалий, обеспечивает баланс между точностью обнаружения малозаметных атак типа SlowLoris, RUDY
и вычислительной эффективностью.

Обеспечение совместимости адаптивных карт Кохонена с четырьмя классами систем обнаружения вторжений требует разработки унифицированного промежуточного слоя, абстрагирующего особенности конкретной платформы. Такой слой должен обеспечивать преобразование входных данных в стандартный формат векторов признаков, управление жизненным циклом карты (инициализация, обучение, адаптация топологии, переобучение) и передачу результатов анализа в родную систему в формате, соответствующем её интерфейсам. Критически важным становится поддержка как зарубежных архитектур x86-64 и ARM, так и отечественных процессорных платформ через оптимизированные библиотеки линейной алгебры. Только при условии решения этих задач адаптивные самоорганизующиеся карты с динамической топологией смогут занять устойчивое место в многоуровневой архитектуре кибербезопасности, обеспечивая надёжное выявление малозаметных атак в условиях гетерогенной инфраструктуры.

Источники и литература

1) Аль-Тамими М., Хассан М.Б., Пазников А.А., Аль-Хайкани М.Н., Альбадрави Е.Б. Обзор систем обнаружения вторжений // Известия СПбГЭТУ «ЛЭТИ». 2024. Т. 17, № 4. С. 30–41.

2) Долгачев М.В., Москвичев А.Д., Москвичева К.С. Обнаружение атак на веб-приложение с помощью самоорганизующихся карт Кохонена // Вопросы кибербезопасности. 2024. № 1(59). С. 38–44.

3) Слесарчик К.Ф. Метод обнаружения низкоинтенсивных распределенных атак отказа в обслуживании со случайной динамикой характеристик фрагментации и периодичности // Вопросы кибербезопасности. 2018. № 1(25). С. 19–27.