УДК 004.891:004.056

РАЗРАБОТКА МУЛЬТИАГЕНТНОЙ СИСТЕМЫ ДЛЯ АНАЛИЗА ЗАЩИЩЕННОСТИ И КОНТРОЛЯ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ

Илиев И.И. (ИТМО), **Диденко Д.Э.** (ИТМО)
Научный руководитель – старший преподаватель ФПИиКТ Русак А.В. (ИТМО)

Введение. В настоящее время вопросы безопасности веб-приложений продолжают набирать популярность. Традиционные средства защиты, такие как межсетевые экраны уровня приложений (WAF) и сканеры уязвимостей, опираются на сигнатурные методы и статические правила, что делает их недостаточно эффективными против сложных целевых атак [1]. Кроме того, существующие инструменты не обеспечивают требуемую скорость реагирования на инциденты. Зарубежные исследования указывают на переход к автономным мультиагентным системам, способным не только обнаруживать, но и самостоятельно устранять угрозы, оповещая операторов SOC [2]. В отечественной практике также наблюдается рост интереса к интеллектуальным системам защиты, однако большинство решений всё ещё представляют собой разрозненные инструменты, не объединенные в единую систему [3]. В связи с этим, разработка интегрированной мультиагентной системы, объединяющей сбор данных, анализ уязвимостей и автоматическое реагирование, является актуальной задачей создания самоадаптирующейся защиты веб-ресурсов.

Основная часть. В качестве решения поставленной проблемы в работе предлагается подход, основанный на построении мультиагентной системы, интегрируемой непосредственно в архитектуру веб-приложения. Функционирование системы строится на последовательном взаимодействии трех основных интеллектуальных модулей. На первом этапе агент-наблюдатель осуществляет непрерывный мониторинг входящего HTTP-трафика и системных логов в режиме реального времени, выполняя предварительную фильтрацию и выделение аномалий для снижения нагрузки на систему. Выявленные подозрительные данные передаются агенту-аналитику, который проводит проверку инцидентов, используя контекстный анализ и модели машинного обучения для точного определения вектора атаки и минимизации ложноположительных срабатываний. На основе сформированного вердикта агент реагирования принимает финальное решение, обеспечивая не только мгновенную блокировку угроз, но и генерацию отчетов с рекомендациями по исправлению конкретных фрагментов уязвимого кода. Дополнительно архитектура системы включает ряд вспомогательных агентов, обеспечивающих поддержку сопутствующих задач и повышающих общую адаптивность и устойчивость механизма защиты.

Выводы. Разработанная мультиагентная система решает проблему низкой эффективности традиционных сигнатурных методов противодействия целевым атакам. Кроме того, автоматизация процессов обнаружения и реагирования решает проблему оперативной обработки инцидентов, минимизируя нагрузку ответственных лиц и устраняя задержки, свойственные ручному управлению разрозненными средствами защиты.

Список использованных источников:

1. Защита веб-приложений в 2024 году: аналитический обзор [Электронный ресурс] // Anti-Malware.ru: информационно-аналитический центр. — 2024. — Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/Web-Apps-Security-AMLive-2024 (дата обращения: 12.02.2026).
2. Hua Y. A Multi-Agent System for Cybersecurity Threat Detection and Correlation Using Large Language Models / Y. Hua, F. Li // IEEE Access. — 2025. — Vol. 13. — P. 150–162.
3. Прогноз развития рынка кибербезопасности в Российской Федерации на 2025–2030 годы [Электронный ресурс]: аналитический доклад / Фонд «Центр стратегических разработок». — Москва: ЦСР, 2024. — 60 с. — Режим доступа:

https://www.csr.ru/ru/research/prognoz-razvitiya-rynka-kiberbezopasnosti-v-rf-na-2025-2030-gody/ (дата обращения: 12.02.2026).

Автор _____ Илиев И.И.

Научный руководитель _____ Русак А.В.