УДК 004.056

Разработка алгоритма автоматизированного тестирования на проникновение сетевых инфраструктур на основе машинного обучения с подкреплением

Шерягин М.А. (ИТМО)
Научный руководитель – кандидат технических наук, доцент Менщиков А.А. (ИТМО)

Введение. Тестирование сетевых инфраструктур на проникновение становится особенно важным в современны условиях роста киберугроз [1], связанных с интенсивно развивающейся сферой информационных технологий. Сетевые инфраструктуры уникальны из-за различий в топологии, конфигурации оборудования, а также в политиках безопасности и в многообразии протоколов. Традиционные автоматизированные методы тестирования имеют ограничения по заранее заданным правилам и шаблонам [2]. Следовательно, они недостаточно гибки и неспособны адаптироваться к специфике каждой системы. А использование ручного тестирования требует зачастую повышения трудозатрат. В данном исследовании предлагается разработка алгоритма автоматизированного тестирования, основанного на методах машинного обучения с подкреплением, что позволит оптимизировать процесс обнаружения уязвимостей и обеспечить более оперативное реагирование на потенциальные атаки.

Основная часть.

1) Анализ существующих методов тестирования на проникновение. Рассмотрены классические подходы, автоматизированные сканеры уязвимостей и динамические методы эмуляции атак, выявлены их преимущества и ограничения в условиях современных сетевых инфраструктур.
2) Применение методов машинного обучения с подкреплением в информационной безопасности. Описаны основные принципы обучения с подкреплением, постановка задачи тестирования в виде оптимизационной проблемы, выбор функции вознаграждения и использование алгоритмов Q-learning и DQN для формирования адаптивной стратегии атак [3].
3) Разработка алгоритма автоматизированного тестирования. Представлена архитектура системы, включающая модули генерации тестовых сценариев, анализа результатов и корректировки стратегии на основе обратной связи. Описаны этапы обучения агента, интеграция с существующими инструментами тестирования и особенности реализации в реальных условиях эксплуатации сетевых инфраструктур [4].
4) Экспериментальное исследование и оценка эффективности. Проведено моделирование различных тестовых сред, сравнительный анализ работы алгоритма и традиционных методов, что позволило оценить потенциал повышения эффективности обнаружения уязвимостей и сокращения времени тестирования.

Выводы. Разработанный алгоритм автоматизированного тестирования на проникновение, основанный на методах машинного обучения с подкреплением, продемонстрировал достаточно высокую эффективность в условиях моделирования сетевых инфраструктур. Адаптивная стратегия тестирования позволяет оперативно реагировать на изменения конфигураций систем и минимизировать вероятность пропуска критических уязвимостей. Результаты экспериментов подтверждают перспективность применения данного подхода при проведении тестирования сетевых инфраструктур для снижения трудозатрат и повышения качества работы.

Список использованных источников:

1. Готовы ли российские компании противостоять кибератакам? [Электронный ресурс] / Positive Technologies. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/are-

russian-companies-well-prepared-to-fend-off-cyberattacks (дата обращения: 22.02.2025).
2. Metasploit Unleashed [Электронный ресурс] / OffSec. – Режим доступа: https://www.offsec.com/metasploit-unleashed/introduction (дата обращения 22.02.2025).
3. Reinforcement Learning: An Overview. / arXiv.org e-Print archive – arXiv:2412.05265 [cs.AI].
4. Gamifying machine learning for stronger security and AI models [Электронный ресурс] / Microsoft Security. – Режим доступа: https://www.microsoft.com/en-us/security/blog/2021/04/08/gamifying-machine-learning-for-stronger-security-and-ai-models/ (дата обращения 22.02.2025).