**УДК 004.056.53**

# Разработка метода автоматизированного Тестирования на проникновение инфраструктуры

**Пограновский Г.И.** (ВКА), **Калашников П.Д.** (ВКА)
**Научный руководитель – кандидат технических наук, Киселёв А.Н.** (ВКА)

**Введение.** В современных условиях проблема обеспечения информационной безопасности организаций становится все более актуальной. Современные информационные системы сталкиваются с постоянным ростом числа уязвимостей. Одним из наиболее эффективных способов выявления и устранения уязвимостей в сетях является проведение тестирования на проникновение [1]. Однако традиционные методы тестирования на проникновение требуют значительных временных и человеческих ресурсов, что затрудняет их регулярное применение. Актуальной задачей является разработка автоматизированных систем, способных воспроизводить процесс тестирования на проникновение для анализа сетевых топологий и выявления потенциальных векторов атак с минимальным вмешательством человека. Исследования в этой области за рубежом и в России показывают, что использование технологий искусственного интеллекта, а именно методов и алгоритмов машинного обучения может значительно повысить эффективность подобных систем.

**Основная часть.** Предлагаемый подход заключается в разработке системы автоматизированного анализа логической топологии компьютерных сетей. Система предназначена для проведения предварительного анализа потенциальных векторов атак и оптимизации процесса тестирования на проникновение.

Решение основано на следующих подходах:

1) Использование логического анализа для построения модели компьютерной сети – цифрового двойника [2], включающей данные о топологии, перечень уязвимостей обнаруженных хостов в сети, возможных способов их эксплуатации с анализом негативных последствий и рекомендации по их автоматическому устранению.

2) Применение алгоритмов оптимизации для определения кратчайших и наиболее эффективных векторов атак в компьютерной сети при проведении тестирования [3].

Преимуществом такого подхода является возможность детального анализа компьютерной сети на этапе планирования тестирования на проникновение без взаимодействия с реальной инфраструктурой, с использованием так называемого цифрового двойника. Это исключает вероятность случайного негативного воздействия на систему и позволяет сосредоточиться на всестороннем анализе уязвимостей. Разработанное решение может быть адаптировано для интеграции и совместного использования с существующими базами данных уязвимостей и фреймворками.

**Выводы.**

Автоматизация процесса тестирования на проникновение с использованием логического анализа позволяет сократить время на анализ сложных сетевых топологий, позволяя специалисту в области тестирования на проникновение сосредоточиться на выполнении более трудоемких задач, требующих нестандартных и творческих подходов, а также значительно улучшить качество результатов.

**Список использованных источников**:

1. Matthew Hickey, Jennifer Arcuri. Hands on Hacking .Become an Expert at Next Gen Penetration Testing and Purple teaming. – Wiley, 2020. c.15-18.
2. F. Tao, J. Cheng, Q. Qi et al, (2018). Digital twin-driven product design, manufacturing and service with big data. Int J Adv Manuf Technol, 94:3563–3576.
3. Филимонов, А. Б. Методы оптимизации : учебное пособие / А. Б. Филимонов, Н. Б. Филимонов. — Москва : РТУ МИРЭА, 2021. — 90 с. — Текст : электронный // Лань : электронно-библиотечная

система. — URL: https://e.lanbook.com/book/218639 (дата обращения: 26.01.2025). — Режим доступа: для авториз. пользователей. — С. 39.).