**УДК 004.8**

# РАЗРАБОТКА ГИБРИДНОГО АЛГОРИТМА LLM И FP-GROWTH ДЛЯ ПРОГНОЗИРОВАНИЯ ТЕХНИК MITRE ATT&CK.

**Горбунов К.Д.** (ИТМО)

**Научный руководитель – кандидат физико-математических наук, доцент Иванов С.Е.** (ИТМО)

**Введение.** По оценкам профильных порталов число инцидентов в сфере информационной безопасности за последние несколько лет растет по экспоненте [1]. Однако, атака не происходит в моменте. Атака – это всегда последовательность действий, которая может длиться минуты, дни, месяцы и даже годы.

В таких условиях особенно важно уметь прогнозировать дальнейшие шаги злоумышленников. Одним из способов превентивной защиты от атак является пентест информационных систем [2]. Основной недостаток пентеста – временные ресурсы. Пентест необходимо проводить перед каждым обновлением, что растягивает сроки запуска проектов.

Процесс пентеста все же можно автоматизировать за счет внедрения в него LLM-моделей. Недавнее исследование компании XBOW показало, что современные LLM-модели становятся все более эффективными для поиска уязвимостей [3]. Однако, модель все же ограничена тем набором данных, на котором она была обучена, а кибератаки модифицируются постоянно.

В такой ситуации актуальным становится гибрид LLM-модели и релевантных данных, которые она будет получать на вход вместе с исходным запросом [4].

**Основная часть.** Целью исследования является разработка гибридного LLM-агента, использующего ассоциативные правила для прогнозирования техник MITRE ATT&CK.

Для успешного достижения цели работы были определены следующие задачи:

1) Обзор литературы по LLM-моделям и методам построения ассоциативных правил;
2) Формирование набора данных о киберинцидентах для валидации работы алгоритма;
3) Определение методологии исследования;
4) Анализ эффективности работы алгоритма, доработка параметров моделей для достижения наилучших результатов;
5) Валидация полученных результатов.

**Выводы.** Разработан гибридный алгоритм LLM и FP-Growth для прогнозирования векторов атак злоумышленников на информационные системы. Определены оптимальные параметры прогнозных моделей, позволяющие достичь наибольшей точности прогнозов.

**Список использованных источников**:

1. Kalashnikov A.O., Anikina E.V., Ostapenko G.A., Borisov V.I. The impact of new technologies on the information security of critical information infrastructure. Information and Security. 2019. Vol. 22. No. 2.

2. Sarkar, S.: A Study on Cybersecurity Standards for Power Systems. In: Advanced Power System Standards and Practices. pp. 429–450. (2023). ISBN: 978-3-031-20359-6. https://doi.org/10.1007/978-3-031-20360-2_18.

3. XBOW Unleashes GPT-5’s Hidden Hacking Power, Doubling Performance. – Online resource // Publisher: https://xbow.com/ URL: https://xbow.com/blog/gpt-5 (accessed 20.02.2026).

4. Sreejith, A., Swarup, K.: MITRE ATT&CK for Smart Grid Cyber-Security. In: Smart Grid Security and Privacy. pp. 59–73. (2024). ISBN: 978-981-97-1301-1. https://doi.org/10.1007/978-981-97-1302-8_5.