Таким образом, предложенная модель позволяет перейти от формальной проверки сложности к оценке практической стойкости пароля. Её применение повышает качество выявления слабых паролей и делает обратную связь более содержательной. Перспективы развития связаны с расширением словарной базы, адаптацией правил и настройкой весов критериев на основе экспериментальных данных.

Список использованных источников

1. Салита Д.С., Удовик А.А. Методы оценки надежности парольных систем // Проблемы правовой и технической защиты информации, 2020, № 8, С. 47-51.

2. Сидоркина И.Г., Михалищев С.В. Совершенствование метода оценки стойкости пароля аутентификации пользователя компьютерных систем на основе использования известных уязвимостей // Программные продукты и системы, 2024, № 4, С. 547-553.

3. Рекомендательная система проверки стойкости паролей [Электронный ресурс]. GitHub, 2026. URL: https://github.com/raOvOen/RPS-GUI/ (дата обращения: 10.03.2026).

Иванов Александр Григорьевич, аспирант РГГУ, alexandr.link.ivanov@gmail.com.
Лось Владимир Павлович, д.в.н., профессор, РГГУ, los-vladimir@yandex.ru

УДК 004.056:004.89

ВЛИЯНИЕ ТОПОЛОГИИ СЕТИ НА РАСПРОСТРАНЕНИЕ ДЕЗИНФОРМАЦИИ СРЕДИ LLM-АГЕНТОВ

В.П. Лось, А.К. Шувалов
Российский государственный гуманитарный университет, г. Москва

Дезинформация является одной из главной угроз современного общества. Проблемы и вызовы нового вектора атаки активно обсуждаются на международной арене. Вызвано это тем, что широкое распространение получили социальные сети, которые являются одним из главных средств распространения подобного контента. Также упростилось и создание материалов, так как теперь для этого используются LLM, качество генерации текста которых увеличиваются и становится почти не отличимо от написанного человеком [1]. Для анализа и защиты от подобных угроз активно используются LLM-агенты, которые способны воспринимать текст на естественном языке, рассуждать и принимать решения о передачи информации другим участникам сети [2, 3]. В работе рассматривается влияние выбора топологии сети на характер распространения дезинформации в системах с LLM-агентами.

К классическим моделям распространения информации можно отнести:

- SIR;
- Каскадная модель;
- Модели динамики мнений.

Однако их ограничение в том, что они оперируют четко заданными правилами и скалярными величинами, для принятия решения, не учитывая внешний фон, рассуждения самого актора, что отличается от поведения человека [4]. LLM-агенты лишены этого недостатка, так как оперируют прошлыми знаниями и подстраиваются под окружающую среду, что отражается на решении агента о том, верить полученной информации, отвергнуть и передать ли ее дальше [5].

В современных работах по LLM-агентным социальным сетям используются четыре основных класса топологий:

- Случайный граф Эрлеша-Реньи. Задаются равновероятные связи между узлами. В таких сетях дезинформация распространяется равномерно, без явных локальных кластеров [6];
- Граф малого мира Уоттса-Строгатца. Высокая степень кластеризации с короткими путями. Такая топология ближе всего к реальным социальным сетям и создает условия для создания эхо-камер (плотный кластер из пользователей, где информация активно передается между одним наборов узлов усиливая друг друга) [6, 7];
- Безмасштабные сети Барабаши-Альберт. Характеризуется наличием узлов с аномально большим числом связей. Воздействие на такое узел приводит к активном распространению дезинформации [8].
- Реальные сетевые структуры. Используются для валидации моделей, основаны на данных реальных пользователей социальных сетей.

Настоящие исследования показывают, что в зависимости от выбора топологии графа для построения социальной сети, можно получить различную степень поражения узлов. В одной из работ были проверены все 4 варианта распространения информации, было получено, что степень вовлеченности узлов колеблется от 0 до 83%, при этом, данные показатель зависит исключительно от выбора сети. В безмасштабных сетях наиболее эффективно оказалось воздействовать на 2-3 аномальных узла с большим числом связей, что уже привело к широкому распространению дезинформации. В графах малого мира было получено, что эхо-камеры формируется на 40% быстрее, чем в случайных графах, при этом, формирование такой изолированной единицы, которая содержит 5 и более активных участников, приводит к отверганию корректирующей информации в 78% случаев, тогда как в их отсутствии, отдельные участники принимают ее в 61% случаев.

При анализе распространения дезинформации необходимо учитывать и динамические факторы, которые также оказывают сильное влияние. К ним можно отнести рекомендательные алгоритмы социальных сетей, которые выявляют паттерн и предлагают только ту информацию, с которой согласен пользователь. Также LLM-агенты способны сами разрывать связи с другими узлами сети, если те не согласны с их мнением [9].

В итоге, если рассматривать данный материал с позиции информационной безопасности, то можно сделать вывод, что безмасштабные сети наиболее уязвимы к целенаправленным атакам на

аномальные узлы, сети малого мира подвержены активному формированию эхо-камер. В таких топологиях наиболее эффективным способом защиты будет, обеспечение безопасности аномального узла для безмаштабных и выстраивание мостов между кластерами для сетей малого мира. Исходя из понимания того, что структура социальной сети является одним из ключевых факторов, который влияет на распространение дезинформации можно сделать вывод, что платформы, основанные на LLM-агентах, способны предоставить исследователям площадку для проведения симуляционных атак для нахождения слабых мест и выстраивании процесса защиты в период информационных войн, что делает их перспективным направлением в области информационной безопасности.

Список использованных источников

1. Goldstein, J.A. et al. Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations // arXiv:2301.04246. — 2023.

2. Park, J.S. et al. Generative Agents: Interactive Simulacra of Human Behavior // Proc. of UIST. — ACM, 2023.

3. Yang, Z. et al. OASIS: Open Agent Social Interaction Simulations with One Million Agents // arXiv:2411.11581. — 2024.

4. Губанов, Д.А. Социальные сети: модели информационного влияния, управления и противоборства / Д.А. Губанов, Д.А. Новиков, А.Г. Чхартишвили. — М.: Физматлит, 2010. — 228 с.

5. Liu, Y. et al. From Skepticism to Acceptance: Simulating the Attitude Dynamics Toward Fake News // Proc. of IJCAI. — 2024.

6. Hu, T. et al. Simulating Rumor Spreading in Social Networks using LLM Agents // Proc. of AAAI Workshop WMAC. — 2025.

7. Wang, C. et al. Decoding Echo Chambers: LLM-Powered Simulations Revealing Polarization in Social Networks // Proc. of COLING. — 2025.

8. Buitrago López, A. et al. Agent-based simulation of online social networks and disinformation // Information Sciences. — 2025.

9. Gu et al. Large Language Model Driven Agents for Simulating Echo Chamber Formation // arXiv:2502.18138. — 2025.

Лось Владимир Павлович, д.в.н., профессор, РГГУ, los-vladimir@yandex.ru
Шувалов Александр Константинович, аспирант, РГГУ, mr.sasha.shuv@gmail.com

УДК 004.492.3

МОДУЛЬНО-ИЗОЛИРОВАННАЯ ИЕРАРХИЯ ПОЛИТИК БЕЗОПАСНОСТИ МЕЖСЕТЕВЫХ ЭКРАНОВ КАК МЕХАНИЗМ ЛОКАЛИЗАЦИИ ОШИБОК КОНФИГУРАЦИИ

Е.К. Литинская, Н.В. Кучкарова
Уфимский университет науки и технологий, г. Уфа

Ключевые слова: межсетевой экран, иерархия политик, эшелонированная защита, локализация ошибок.