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.

Современные корпоративные сети защищаются комплексом средств, однако основой периметра остаются межсетевые экраны (МЭ). В реальных конфигурациях число правил исчисляется тысячами, где одно ошибочное изменение способно непреднамеренно открыть сквозной путь доступа [1]. Общий принцип противодействия – Defence in Depth (эшелонированная защита) – обычно применяется на уровне инфраструктуры, но не формализован для структуры правил МЭ [2]. Существующие решения (распределенные МЭ, иерархические политики) обеспечивают защиту за счет архитектурной разнородности, но не гарантируют логическую изоляцию правил [3, 4]. Это сохраняет риск сквозного распространения ошибок конфигурации. Исследования трехмодульной архитектуры политик безопасности [5] и совершенствованию спецификации политики для практических систем контроля доступа [6] закрепляет изоляцию модулей, фиксированных алгоритмом подхода. Проблема остается в фиксированных модулях.

В работе предлагается конкретизация принципа эшелонирования через модульно-изолированную иерархию политик МЭ. Вводятся четыре независимых уровня, применяемых последовательно. Ключевым требованием является свойство монотонного ужесточения: каждый уровень может только сузить, но не расширить разрешённый доступ, определённый на предыдущем уровне. Гипотеза исследования заключается в том, что при соблюдении изоляции уровней ошибка конфигурации на одном из них концептуально ограничивается данным уровнем и не распространяется на остальные.

Для демонстрации подхода рассмотрен фрагмент сети с сегментами: внешний периметр (DMZ), прикладные серверы и базы данных. Политики структурируются по четырём уровням (табл. 1).

Таблица 1 – Пример реализации модульно-изолированной иерархии политик безопасности

Уровень	Тип политики	Функциональное назначение	Пример правила
1	Периметр	Доступ из внешних сетей	Разрешить HTTP/HTTPS к DMZ. Запретить прочее.
2	Сетевая сегментация	Маршруты между сегментами	Разрешить DMZ к «Приложения. Запретить к «БД».
3	Прикладной уровень	Контроль протоколов приложений	Разрешить SQL-запросы. Запретить управление ОС.
4	Идентификация и доступ	Доступ на целевой системе	Доступ к БД только с IP сервера приложений и по учётным данным.

Реализация иерархии предполагает разнородность средств: уровень периметра обеспечивается NGFW, сегментация – сетевым оборудованием, прикладной уровень – WAF, идентификация – хостовыми экранами. Такая

разнородность гарантирует, что уязвимость инструментария одного уровня не приведёт к автоматическому снятию ограничений на последующих. Ошибка конфигурации (например, избыточное разрешение на уровне 2) не приводит к компрометации ресурса, так как уровни 3 и 4 сохраняют ограничивающие функции.

Предложенная модель обладает рядом ограничений. Во-первых, повышение эксплуатационной сложности: разделение политики требует координации настроек на разнородных компонентах и валидации на всех уровнях. Во-вторых, накладные расходы на обработку трафика: последовательная фильтрация вносит задержку, что критично в высоконагруженных сегментах.

Таким образом, подход представляет компромисс между уровнем защищённости и сложностью управления. Выявленные ограничения связаны с организационными факторами и высокой ресурсоемкостью. Научная новизна заключается не в предложении новой сетевой топологии, а в разработке методологии описания политик безопасности, гарантирующей логическое эшелонирование. Дальнейшие исследования направлены на количественную проверку гипотезы и внедрение средств автоматизированного управления политиками.

Список использованных источников

1.Al-Shaer E. Quantitative Analysis of Firewall Policy Anomalies / E. Al-Shaer, Q. Hamed // IEEE Transactions on Network and Service Management. – 2009. – Vol. 6, No. 2.

2.Scarfone K. Guidelines on Firewalls and Firewall Policy : NIST Special Publication 800-41 Rev. 1 / K. Scarfone, P. Hoffman. – Gaithersburg : NIST, 2009.

3.Bellovin S. M. Distributed Firewalls / S. M. Bellovin // Login: The USENIX Magazine. – 1999. – Vol. 24, No. 7.

4.Lee J. H. A Study on Hierarchical Policy Model for Managing Heterogeneous Security Systems / J. H. Lee, S. U. Shin, K. Y. Yoo // Journal of the Korea Institute of Information Security & Cryptology. – 2011. – Vol. 21, No. 6.

5.Chen H. Tri-Modularization of Firewall Policies / H. Chen, O. Chowdhury, N. Li [et al.] // Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC '12). – New York : ACM, 2012.

6.Chen H. Improving the Policy Specification for Practical Access Control Systems / Haining Chen. – Purdue University : ProQuest Dissertations & Theses, 2017.

Литинская Екатерина Константиновна, студ. каф. вычислительной техники и защиты информации, litkaterina2312@gmail.com.
Кучкарова Наиля Вакилевна, к.т.н., доцент каф. вычислительной техники и защиты информации, , nailya_kuchkarov@mail.ru.