

ОПРЕДЕЛЕНИЕ МЕСТА ВНЕДРЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ С ПРИМЕНЕНИЕМ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

О.Е. Евсеева¹, Л.И. Сурова¹, Е.Г. Убанеева¹

¹Федеральный научно-производственный центр акционерное общество
«Научно-производственное объединение «Марс», г. Ульяновск
e-mail: evseeva-2507@mail.ru

Аннотация

В научной статье представлен комплексный анализ трехуровневой иерархической топологии в случаях деградации некоторого набора каналов связи между сетевым оборудованием. В основу разрабатываемых моделей положены методы теории графов и мер центральности. Это позволяет оперативно выявить наиболее значимые узлы сетевой топологии, которые рассматриваются в качестве потенциальных точек интеграции систем обнаружения вторжений и локальных вычислительных сетей.

Ключевые слова: системы обнаружения вторжений, имитационное моделирование, локальные вычислительные сети, теория графов, меры центральности.

Введение

Для обеспечения стабильности, безопасности локальных вычислительных сетей, быстрого обнаружения инцидентов безопасности и принятия соответствующих мер используются различные инструменты, необходимые для захвата трафика.

Одним из таких инструментов являются системы обнаружения вторжений (СОВ) уровня узла и сети. Внедрение СОВ, как средства анализа сетевого трафика, осуществляется преимущественно на этапе проектирования информационных систем. Таким образом возникает задача оптимального размещения СОВ уровня узла [1].

Постановка задачи

Одним из эффективных способов для решения поставленной задачи является использование алгоритмов центральности, дающих возможность определить значимость каждого узла относительно всей инфраструктуры сети [2]. Мера центральности служит показателем влияния узлов в графе и их воздействия на сетевую инфраструктуру [3]. Авторами предлагается подход, основанный на оценке каждого отдельного узла с помощью базовых мер центральности: степени, близости и промежуточности.

В программной реализации заложен механизм генерации имитационной модели иерархической топологии локальной вычислительной сети (ЛВС), которая обладает следующими особенностями: включает три уровня коммутаторов; имеет отдельные множества коммутаторов для каждого уровня; а также множество автоматизированных рабочих мест (АРМ) и серверов, генерирующих сетевой трафик с различной интенсивностью.

При моделировании деградации ЛВС рассматриваются случаи потери каждой связи в сети, далее – пары ребер и так вплоть до состояний сети, сохраняющих хотя бы один функционирующий путь между иерархическими уровнями сети. Методика исследования предполагает полный перебор комбинаций деградации топологии для оценки устойчивости сети.

В качестве порогового значения используется 75-й перцентиль, то есть узлы, чьи показатели центральности превышают данный порог, классифицируются как значимые, поскольку их значения превосходят показатели 75% наблюдений в выборке [4].

Для исследования предполагаемого подхода используем сетевую топологию, графовая модель которой представлена на рисунке 1. В рамках работы было организовано 13 сценариев деградации ЛВС.

Для верификации объективности предложенной модели в ходе экспериментальных исследований осуществлялся мониторинг динамики сетевого трафика. На представленных гистограммах (рисунки 2-3) используется две оси: левая отображает значения ключевых метрик центральности, а правая – суммарный объём передаваемого трафика в исследуемом сегменте сети.

Анализ экспериментальных данных выявил устойчивую корреляционную зависимость: по мере увеличения числа удалённых рёбер наблюдается монотонное снижение значений всех рассматриваемых характеристик. Данный процесс сопровождается пропорциональным уменьшением общего объёма сетевого трафика.

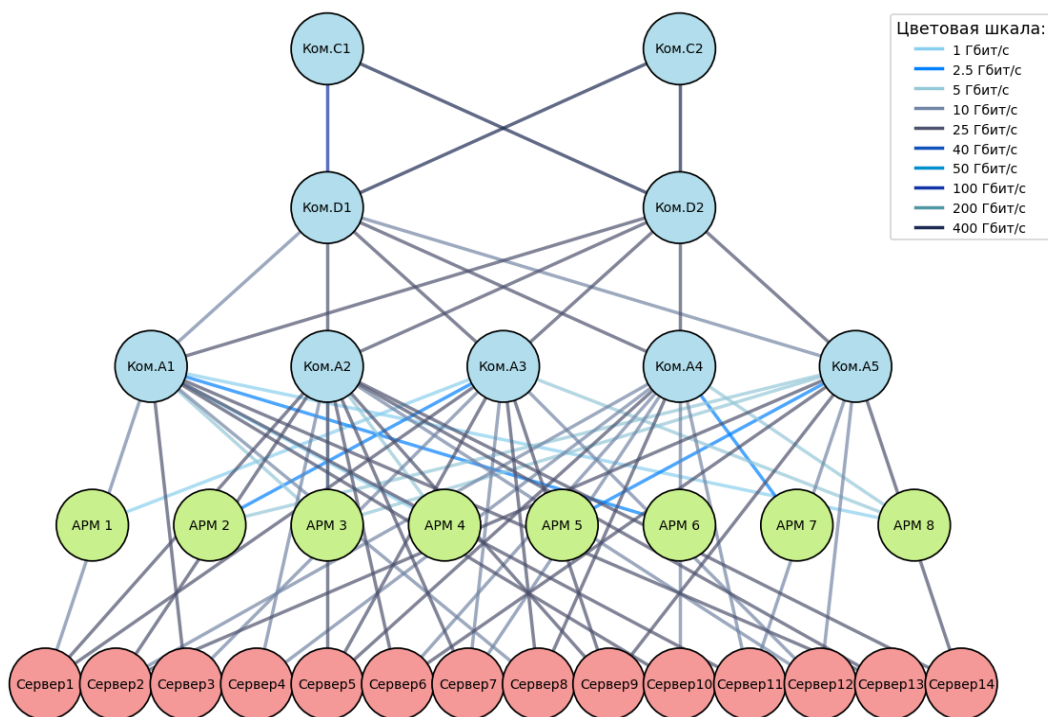


Рисунок 1 – Граф исследуемой сети

Выявленная тенденция является подтверждением адекватности и высокой степени реалистичности предлагаемой имитационной модели. Она достоверно

воспроизводит процессы деградации связности и функциональности, характерные для реальных сетевых инфраструктур при возникновении множественных отказов каналов.

Оценка важности узла сетевой инфраструктуры топологии ЛВС

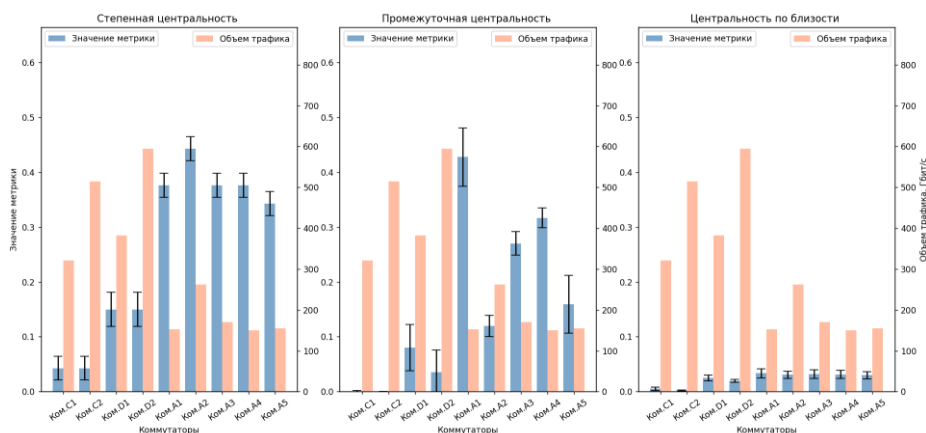


Рисунок 2 – Гистограммы при деградации 5 рёбер

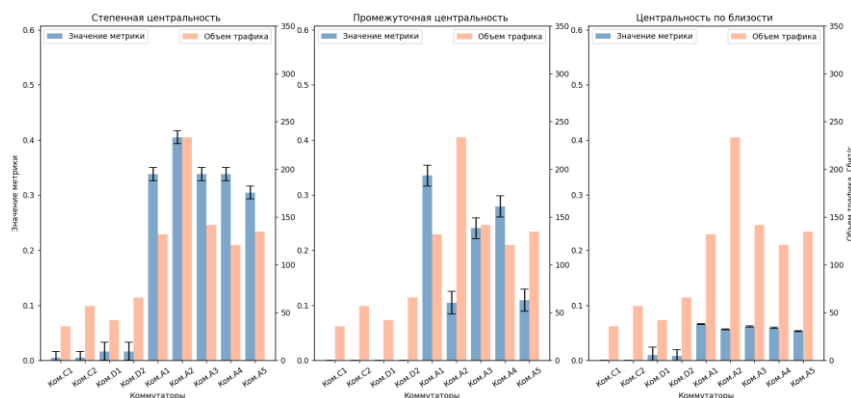


Рисунок 3 – Гистограммы при деградации 13 рёбер

При выявлении оптимальных узлов для внедрения СОВ с применением порогового значения равного 75-ому перцентиллю, было выявлено, что узлы Ком.А1, Ком.А3 и Ком.А4 являются критически важными, Ком.А2 – локальным, превышая пороговое значение по степенной центральности, все остальные узлы – низко приоритетные (рисунок 4).

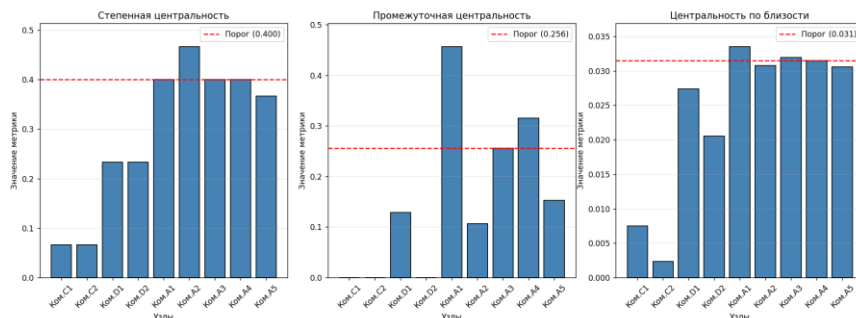


Рисунок 4 – Гистограммы пороговых значений

Так, определение порогового значения зависит от конкретной решаемой задачи и требует уровня детализации. Варьируя данный порог, можно гибко настраивать количество и состав ключевых узлов, подлежащих внедрению СОВ.

Заключение

В данной работе представлен разработанный подход, позволяющий на основе расчета центральных характеристик определить оптимальное местоположение для внедрения СОВ в сетевую инфраструктуру. В рамках исследования применяются алгоритмы расчёта мер центральности, которые количественно характеризуют значимость каждого узла для функционирования всей топологии.

Список использованных источников

1. Евсеева, О. Е. Имитационная модель деградации сети передачи данных как инструмент оценки важности узла для функционирования сетевой инфраструктуры / О. Е. Евсеева, С. А. Дрягин, А. С. Корсунский [и др.] // Автоматизация процессов управления / Automation of Control Processes. – 2026. – Т.1, № 83.
2. Антонов, А. В. Сравнительный анализ мер центральности для выявления ключевых агентов в сети региональных маркетинговых сообществ / А. В. Антонов, Р. С. Стирманова // Моделирование и анализ данных. – 2025. – Т. 15, № 2. – С. 7–26.
3. Косимова, М. Ш. кизи. Приложения теории графов в компьютерной сетевой безопасности / М. Ш. кизи Косимова // Eurasian Journal of Academic Research. – 2024. – Т. 4, № 6 – С. 24–27.
4. Аванесов, В. Структурные характеристики вариационного ряда: применение квантилей для интерпретации тестовых результатов / В. Аванесов // Педагогические измерения. – 2010. – № 1. – С. 104–116.

DEFINITION OF THE PLACE OF IMPLEMENTATION OF THE SYSTEMS OF DETECTION OF INTRUSIONS IN LOCAL COMPUTER NETWORKS WITH THE APPLICATION OF SIMULATION MODELING

O.E. Evseeva¹, L.I. Surova¹, E.G. Ubaneeva¹

¹Federal Research and Production Center Joint Stock Company

"Mars Scientific and Production Association", Ulyanovsk

e-mail: evseeva-2507@mail.ru

Abstract

The scientific article presents a comprehensive analysis of a three-level hierarchical topology in cases of degradation of a certain set of communication channels between network equipment. The developed models are based on the methods of graph theory and centrality measures. This allows you to quickly identify the most significant nodes of the network topology, which are considered as potential integration points for intrusion detection systems and local area networks.

Keywords: intrusion detection systems, simulation modeling, local area networks, graph theory, centrality measures.