МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»

Кафедра дискретной математики и информационных технологий

МОДЕЛИРОВАНИЕ КАСКАДНЫХ ОТКАЗОВ В БЕЗМАСШТАБНЫХ СЕТЯХ И ОЦЕНКА ИХ УСТОЙЧИВОСТИ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студентки 4 курса 421 группы
направления 09.03.01 — Информатика и вычислительная техника
факультета КНиИТ
Останиной Анастасии Дмитриевны

Научный руководитель
доцент, к. ф.-м. н. ______________ И. Д. Сагаева

Заведующий кафедрой
доцент, к. ф.-м. н. ______________ Л. Б. Тяпаев

Саратов 2026

ВВЕДЕНИЕ

Безмасштабные сети, характеризующиеся степенным распределением степеней узлов и наличием небольшого числа высокосвязанных узлов (хабов), широко используются для моделирования интернета, энергосистем, социальных и биологических сетей. Отказ даже одного узла в безмасштабной сети может привести к каскадному эффекту – цепной реакции разрушений из-за перегрузки соседних элементов. Изучение устойчивости безмасштабных сетей к различным типам отказов и атак, а также поиск способов ее повышения являются актуальными задачами, имеющими практическое значение для проектирования надежных критических инфраструктур.

Цель работы – смоделировать каскадные отказы в безмасштабных сетях и оценить, как можно повысить их устойчивость.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Проанализировать существующие модели и методы анализа устойчивости сетей.
2. Реализовать модель для имитации каскадных отказов.
3. Провести серию экспериментов для исследования влияния разных параметров сети на устойчивость.
4. Сравнить устойчивость различных типов сетевых структур.
5. Проанализировать возможность применения полученных результатов к реальным сетевым системам.

В работе использованы синтетические сети, сгенерированные по моделям Барабаши–Альберта (BA, $N = 2000$, $m = 3$), Ваттса–Строгаца (WS, $N = 2000$, $k = 6$, $p = 0,1$), Эрдеша–Реньи (ER, $N = 2000$, $p = 6/N$, после выделения гигантской компоненты $N = 1994$), конфигурационная модель (пуассоновское распределение степеней со средним 5, $N = 2000$), а также реальные сети: сеть голосований участников Википедии (Wiki-Vote) и сеть научного соавторства (CA-HepTh) из репозитория SNAP. Все сети приведены к размеру около 2000 узлов. Параметры сетей выбраны так, чтобы обеспечить сопоставимость по плотности связей и размеру.

Работа состоит из введения, четырех глава, заключения, списка использованных источников (50 наименований) и приложения. Первая глава содержит обзор теоретических основ анализа устойчивости безмасштабных сетей.

Во второй главе описана математическая и вычислительная модель каскадных отказов (модель Моттера–Лэя), ее алгоритм и реализация на Python. Третья глава посвящена симуляционному моделированию каскадных отказов на шести типах сетей, анализу полученных результатов и визуализации. В четвертой главе проведено сравнение топологий, выявлены ключевые факторы устойчивости, сформулированы рекомендации по оптимизации сетей и обсуждены ограничения исследования.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первом разделе «Теоретические основы анализа устойчивости безмасштабных сетей» рассмотрены основные понятия теории сложных сетей [1]. В основе математического описания сетевых структур лежит теория графов: граф $\Gamma = (V, E)$ состоит из множества вершин V и множества ребер E. Сложная сеть – это граф с нетривиальными топологическими особенностями, которые не встречаются в простых случайных сетях. Особое внимание уделено безмасштабным сетям, распределение степеней которых подчиняется степенному закону $P(k) \sim k^{-\gamma}$ с показателем $2 < \gamma < 3$ [2, 3]. Это означает, что большинство узлов имеют мало связей, а небольшая часть узлов (хабы) обладает чрезвычайно высокой степенью.

Описаны генеративные модели сложных сетей: модель Эрдеша–Реньи (случайные графы с пуассоновским распределением степеней), модель Барабаши–Альберт (рост и предпочтительное присоединение, дающая степенное распределение $P(q) \sim q^{-3}$) [2, 3], модель Ваттса–Строгаца (сети малого мира с высокой кластеризацией и малой средней длиной пути) [1] и конфигурационная модель (случайные сети с заданным распределением степеней, в работе – пуассоновским со средним 5) [1].

Приведены основные топологические характеристики: распределение степеней $P(q)$, диаметр сети (максимальное расстояние между узлами), коэффициент кластеризации $C_j = t_j/(q_j(q_j-1)/2)$ для узла и средняя кластеризация всей сети [1]. Введены понятия надежности (reliability), устойчивости (robustness) и живучести (resilience) применительно к сетевым структурам [4]. Сеть считается устойчивой к случайным сбоям, если она сохраняет гигантскую компоненту при потере значительной доли узлов [3]. Основным аппаратом анализа структурной устойчивости является теория перколяции, для которой порог перколяции определяется формулой $\phi_c = \langle k\rangle/(\langle k^2\rangle - \langle k\rangle)$ [1].

Рассмотрены модели отказов и атак: каскадные отказы, возникающие из-за внутренних зависимостей, и внешние атаки (случайные и целенаправленные) [4]. Каскадный отказ – это процесс, при котором выход из строя одного элемента приводит к перегрузке соседних и их последующему отказу. Выделены три основных механизма возникновения каскадов: перегрузка (overload), прямые структурные зависимости (interdependencies) и пороговые эффекты [4]. Выполнен обзор существующих моделей каскадных отказов: модель Моттера–Лэя [5] (перераспределение нагрузки, измеряемой посреднической центральностью), модели с пороговыми правилами (bootstrap перколяция, k-ядро), модели взаимозависимых сетей [4]. Показано, что модель Моттера–Лэя наиболее подходит для анализа каскадов, вызванных перегрузкой в одиночных безмасштабных сетях, так как она явно учитывает распределение нагрузки и ограниченную пропускную способность узлов.

Во втором разделе «Математическая и вычислительная модель каскадных отказов» описана формализация модели Моттера–Лэя [5]. Сеть представляется неориентированным графом без петель и кратных ребер. После выделения гигантской компоненты (наибольшего связного подграфа) моделирование каскада проводится только на ней. Для каждого узла i вычисляется начальная нагрузка $L_i(0)$ – нормированная посредническая центральность (betweenness centrality), то есть доля кратчайших путей между всеми парами узлов, проходящих через данный узел. Пропускная способность (емкость) узла задается соотношением $C_i = (1 + \alpha)L_i(0)$, где $\alpha \geq 0$ – параметр толерантности (запас прочности), одинаковый для всех узлов [5].

Каскадный процесс инициируется удалением одного узла (атака). Рассмотрены три сценария:

— случайная атака – инициатор выбирается равновероятно из всех узлов;
— целенаправленная атака – удаляется узел с максимальной начальной нагрузкой $L_i(0)$;
— взвешенно-случайная атака – узел выбирается с вероятностью, пропорциональной его начальной нагрузке.

После удаления инициатора для оставшегося графа пересчитываются кратчайшие пути и текущая нагрузка $L_i(t)$. Если для какого-либо узла $L_i(t) > C_i$, он считается перегруженным и удаляется. Процесс повторяется итерационно (все перегруженные узлы удаляются одновременно на каждом шаге) до тех пор, пока перегруженных узлов не останется [5].

Для оценки последствий каскада используются три метрики: относительный размер гигантской компоненты $S = N_c/N$ (основная метрика), доля отказавших узлов $f = (N - N_f)/N$ и средняя степень выживших узлов $\langle k_{\text{surv}} \rangle$ [1].

Реализован алгоритм моделирования (псевдокод приведен в дипломе). Программная реализация выполнена на языке Python з использованием библиотеки `igraph` [6] (реализация на C, обеспечивающая высокую производительность при многократном вычислении betweenness centrality). Дополнительно задействованы библиотеки `numpy` (случайные числа), `pandas` (агрегация данных), `matplotlib` (визуализация) и `multiprocessing` (параллельные вычисления). Для загрузки реальных сетей из репозитория SNAP используется модуль `requests` и распаковка `gzip`. Субдискретизация реальных сетей до 2000 узлов выполнена методом случайного блуждания (random walk subsampling), сохраняющим локальную структуру.

Основные функции программы: `generate_ba_network`, `generate_ws_network`, `generate_er_network`, `generate_config_network` для генерации синтетических сетей; `load_wiki_network` и `load_ca_heph_network` для загрузки и субдискретизации реальных сетей; `cascade_motter_lai_classic` – реализация итерационного алгоритма каскада; `run_experiment_parallel` – параллельный запуск прогонов через `multiprocessing.Pool`. Всего для каждой из шести сетей, 13 значений α (от 0,1 до 0,7 с шагом 0,05) и трех типов атак выполнено по 10 независимых прогонов. Общее число прогонов составило $6 \times 13 \times 3 \times 10 = 2340$. Параллельные вычисления сократили время расчета с нескольких часов до 30–40 минут на 8-ядерном процессоре.

В третьем разделе «Симуляционное моделирование каскадных отказов» описана процедура генерации шести типов сетей и проведены вычислительные эксперименты. Безмасштабная сеть Барабаши–Альберт (BA) сгенерирована с параметрами $N = 2000$, $m = 3$ [2,3]. Сеть малого мира Ваттса–Строгаца (WS) построена из регулярного кольца $N = 2000$ с $k = 6$ ближайшими соседями и вероятностью переброски ребер $p = 0,1$ [1]. Случайный граф Эрдеша–Реньи (ER) создан с $N = 2000$ и вероятностью связи $p = 6/N$; после выделения гигантской компоненты число узлов составило 1994 [1]. Конфигурационная модель (config) использовала пуассоновское распределение степеней со средним 5 (нулевые степени заменены на единицу), после удаления петель и кратных ребер выделена гигантская компонента [1]. Реальные сети – Wiki-Vote (голосования участников Википедии) [7] и CA-HepTh (соавторство ученых) – загружены из репозитория SNAP, преобразованы в неориентированные, из них выделены гигантские компоненты, а затем методом случайного блуждания выполнена субдискретизация до $N = 2000$ узлов для сопоставимости с синтетическими графами. Итоговые средние степени: BA – около 6, WS – около 12, ER – около 6, config – около 5, Wiki-Vote – около 62, CA-HepTh – около 12.

Параметр толерантности α варьировался от $0,1$ до $0,7$ с шагом $0,05$ (всего 13 значений). Для каждого сочетания сети, α и типа атаки (случайная, целенаправленная по нагрузке, взвешенно-случайная) проведено по 10 независимых прогонов. Общее количество прогонов составило $6 \times 13 \times 3 \times 10 = 2340$.

При случайных атаках все сети, кроме BA, восстанавливаются до относительного размера гигантской компоненты $S > 0,9$ уже при $\alpha = 0,1$; BA требует $\alpha = 0,15$. При целенаправленной атаке на узел с максимальной нагрузкой (targeted_bc) получены следующие минимальные значения α для достижения $S > 0,9$: BA – $0,65$, WS – $0,10$, ER – $0,10$, config – $0,15$, Wiki-Vote – $0,30$, CA-HepTh – $0,35$. При взвешенно-случайной атаке (weighted_random) пороги: BA – $0,30$, WS – $0,10$, ER – $0,15$, config – $0,15$, Wiki-Vote – $0,25$, CA-HepTh – $0,30$.

Таким образом, подтверждена двойственная природа безмасштабных сетей: высокая устойчивость к случайным отказам, но крайняя уязвимость к целенаправленным атакам на хабы [3]. Однородные сети (WS, ER) практически не страдают даже при $\alpha = 0,1$. Конфигурационная модель при малых α может разрушаться из-за случайных флуктуаций, но полностью восстанавливается при $\alpha = 0,15$. Реальные сети Wiki-Vote и CA-HepTh по поведению близки к безмасштабным, однако требуют для восстановления значительно меньший запас прочности ($\alpha = 0,30$ и $0,35$ соответственно), чем модель BA ($0,65$). Это показывает, что реальные топологии могут быть устойчивее идеализированной модели.

Построены графики зависимостей $S(\alpha)$ и $f(\alpha)$ для всех шести сетей. На рис. 1–3 приведены сравнительные графики $S(\alpha)$ для случайной, целенаправленной и взвешенно-случайной атак; на рис. 4–6 – графики доли отказавших узлов $f(\alpha)$. В качестве примера на рис. 7 и 8 показаны зависимости $S(\alpha)$ и $f(\alpha)$ для сети BA. На графиках цветные области соответствуют доверительным интервалам (стандартное отклонение по 10 прогонам). Для случайной атаки в BA сети при малых α интервал широкий, что указывает на бистабильность: исход каскада сильно зависит от того, какой узел отказал первым.

В четвертом разделе «Анализ результатов и пути повышения устойчивости» проведено сравнение различных топологий. На основе полученных пороговых значений α (таблица минимальных α для достижения $S > 0,9$) и графиков $S(\alpha)$ выделены два основных класса сетей: безмасштабные (BA, Wiki-

Vote, CA-HepTh) и однородные (WS, ER, config). Показано, что ключевыми факторами, влияющими на устойчивость к каскадным отказам, являются однородность распределения степеней, плотность связей (средняя степень $\langle k \rangle$) и коэффициент кластеризации C [3, 4].

Установлено, что рост средней степени с 6 (BA) до 12 (CA-HepTh) и до 62 (Wiki-Vote) снижает порог α для целенаправленной атаки с $0,65$ до $0,35$ и $0,30$ соответственно. Высокая кластеризация сети Ваттса–Строгаца ($C \approx 0,38$) обеспечивает исключительную устойчивость при всех типах атак уже при $\alpha = 0,1$. Однородность распределения степеней (отсутствие сверххабов) является важнейшим фактором устойчивости к целенаправленным атакам [3].

Сформулированы практические рекомендации по оптимизации сетей для снижения каскадных эффектов. Для сетей с высоким коэффициентом кластеризации достаточно минимального запаса прочности ($\alpha = 0,1$). В безмасштабных сетях, если избежать формирования хабов невозможно, необходимо предусматривать для них многократное увеличение пропускной способности – запас прочности $\alpha \geq 0,65$. Повышение средней степени (плотности связей) до $\langle k \rangle \approx 10 - 15$ заметно снижает порог восстановления. Даже для сетей с пуассоновским распределением степеней (конфигурационная модель) может потребоваться $\alpha = 0,15$ для подавления случайных флуктуаций, вызывающих каскад.

Пример применения модели к реальным сетям (Wiki-Vote, CA-HepTh) показал, что при целенаправленной атаке порог $S > 0,5$ достигается при $\alpha = 0,30$ для обеих реальных сетей, тогда как для синтетической BA – только при $\alpha = 0,65$. Доля отказавших узлов f при $\alpha = 0,1$ для целенаправленной атаки составляет: BA – $0,676$, Wiki-Vote – $0,690$, CA-HepTh – $0,471$. Это подтверждает, что реальные сети обладают более «дружественной» топологией: хотя начальный отказ хаба вызывает обширные перегрузки, для восстановления связности им требуется значительно меньший запас прочности, чем классической BA-модели.

Отмечено, что модель Моттера–Лэя [5] не учитывает восстановление узлов, веса ребер и неоднородную толерантность; эксперименты проведены для фиксированного размера сети ($N = 2000$) и одиночного начального отказа; реальные сети подвергнуты субдискретизации, что может влиять на некоторые свойства. Перспективные направления: изучение влияния размера сети на пороги α, усложнение модели (введение весов ребер, восстановление узлов, множественные и локализованные атаки), расширение набора реальных сетей (энергосистемы, топология интернета) [4].

ЗАКЛЮЧЕНИЕ

В рамках поставленной цели — моделирования каскадных отказов в безмасштабных сетях и оценки их устойчивости — была последовательно реализована вся совокупность задач дипломной работы. Программно реализована модель Моттера–Лэя, позволяющая имитировать распространение каскадных отказов в сетях различной топологии. На основе этой модели проведены вычислительные эксперименты на шести типах сетей (Барабаши–Альберт, Ваттса–Строгаца, Эрдеша–Реньи, конфигурационной, а также реальных сетях голосований Википедии Wiki-Vote и соавторства ученых CA-HepTh) при трех сценариях инициирования (случайная атака, целенаправленное удаление наиболее нагруженного узла и взвешенно-случайная атака). Всего выполнено 2340 прогонов при варьировании параметра толерантности α от 0,1 до 0,7.

Полученные результаты подтверждают известную двойственность безмасштабных сетей: они демонстрируют высокую устойчивость к случайным отказам, но оказываются крайне уязвимыми при целенаправленном удалении узлов-хабов. Однородные сети (Эрдеша–Реньи, Ваттса–Строгаца) сохраняют связность даже при минимальном запасе прочности, а конфигурационная модель, обладая пуассоновским распределением степеней, при малых α может разрушаться столь же сильно, как и безмасштабные структуры, но полностью восстанавливается при незначительном повышении α. Реальные сети (Wiki-Vote и CA-HepTh) по своему поведению близки к безмасштабным, однако требуют для восстановления значительно меньшего запаса прочности, чем классическая модель Барабаши–Альберт. Высокая кластеризация, характерная для сети Ваттса–Строгаца, обеспечивает исключительную устойчивость при любых типах атак.

Таким образом, ключевыми факторами, влияющими на устойчивость сети к каскадным отказам, являются однородность распределения степеней, плотность связей и уровень кластеризации. Полученные количественные оценки могут служить ориентиром при анализе надежности реальных сетевых инфраструктур.

Основные источники информации:

1. Newman M. Networks: An Introduction. — Oxford : Oxford University Press, 2010. — 772 p.
2. Barabási A.-L. Network Science [Электронный ресурс]. — URL: `https:`

//networksciencebook.com (дата обращения: 15.05.2026).

3. Albert R., Jeong H., Barabási A.-L. Error and attack tolerance of complex networks // Nature. — 2000. — Vol. 406, No. 6794. — P. 378–381.
4. Valdez L. D. et al. Cascading failures in complex networks // Journal of Complex Networks. — 2020. — Vol. 8, No. 2. — P. 1-20.
5. Motter A. E., Lai Y.-C. Cascade-based attacks on complex networks // Physical Review E. — 2002. — Vol. 66, No. 6. — P. 065102.
6. igraph : Python documentation [Электронный ресурс]. — URL: https://python.igraph.org/en/stable/ (дата обращения: 15.05.2026).
7. Wiki-Vote Network [Электронный ресурс] // SNAP (Stanford Network Analysis Project). — URL: https://snap.stanford.edu/data/wiki-Vote.html (дата обращения: 17.05.2026).