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 УСТОЙЧИВОСТИ СЕТЕЙ К СЛУЧАЙНЫМ АТАКАМ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

Студентки 4 курса 421 группы
направления 09.03.01 — Информатика и вычислительная техника
факультета КНиИТ
Замараевой Анастасии Дмитриевны

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

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

Саратов 2025

ВВЕДЕНИЕ

Современное общество всё больше зависит от сложных сетевых структур, таких как интернет, транспортные системы, энергосети и социальные сети. Устойчивость этих сетей к различным видам возмущений, включая случайные атаки и целенаправленные воздействия, является критически важной для их функционирования. Нарушение работы даже небольшого числа узлов или связей может привести к каскадным отказам и значительным социально-экономическим последствиям.

По данным исследований, масштабные сетевые системы демонстрируют уязвимость даже при незначительных возмущениях [1].

Актуальность темы исследования обусловлена необходимостью разработки эффективных методов оценки и повышения устойчивости сетей, особенно в условиях роста их сложности и масштабов. Случайные атаки, в отличие от целенаправленных, могут моделировать непреднамеренные сбои, технические неисправности или внешние воздействия, что делает их изучение важным для обеспечения надёжности сетевых систем [2].

Теория устойчивости сетей базируется на принципах теории графов и статической физики. Ключевыми концепциями являются: уязвимость узлов (влияние степени узла, центральности и кластеризации на устойчивость сети), каскадные отказы и критические пороги [3].

Целью работы является разработка приложения для оценивания устойчивости сети к случайным атакам. Для достижения этой цели поставлены следующие задачи:

1. Рассмотреть существующие модели сетей и методы оценки их устойчивости.
2. Разработать имитационную модель для изучения воздействия случайных атаки на сетевую структуру.
3. Исследовать влияние топологических характеристик сети (степени связности, кластеризации, распределения узлов) на её устойчивость.

В работе применяются методы теории графов, агентного и статистического моделирования, а также анализ устойчивости на основе перколяционной теории.

Структура работы включает введение, три главы, заключение, список использованных источников и приложения. В первой главе "Теоретические

основы исследования устойчивости сетей" рассматриваются теоретические основы исследования устойчивости сетей. Во второй главе "Разработка модели устойчивости сети к случайным атакам" описывается разработка модели и её программная реализация. В третьей главе "Анализ результатов моделирования и оценка устойчивости сети" представлены результаты моделирования и их анализ.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Основное содержание работы включает в себя реферативное изложение сущности работы. Таблицы, графики, диаграммы включаются в автореферат по согласованию с научным руководителем. Рекомендуемый объем данного раздела – не более 8 страниц.

В первом разделе рассматриваются теоретические основы исследования устойчивости сетей, даются основные понятия и определения, необходимые для понимания работы.

В общем смысле, сеть (network) — это совокупность взаимосвязанных элементов, образующих единую структуру [4], [5]. В данной работе рассматриваются сети, которые могут быть представлены в виде графов.

Узел (node, vertex) является основным элементом сети и представляет собой объекты, обладающий определёнными свойствами и способный взаимодействовать с другими узлами.

Ребро(edge, vertex) — это связь между двумя узлами, обозначающая наличие взаимодействия или соединения между ними. Рёбра могут быть ненаправленными, направленными и взвешенными.

Граф (graph) — это математическая абстракция, используемая для представления сети. Граф состоит из множества узлов (вершин) и множества рёбер (связей) между ними. Граф обозначается как $G = (V, E)$, где V — множество узлов, а E — множество рёбер [6].

Существует множество различных типов сетей, отличающихся по структуре, топологии и принципам организации. Наиболее популярными являются следующие типы сетей [7]:

— Случайные сети (Random Networks). Эти сети характеризуются случайным соединением узлов. Классическим примером случайной сети является модель Эрдёша-Реньи (Erdos—Renyi model), в которой каждая пара узлов соединяется с определенной вероятностью. В случайных сетях распределение степеней узлов (количество связей, приходящихся на узел) подчиняется распределению Пуассона.

— Регулярные сети (Regular Networks). В регулярных сетях каждый узел имеет одинаковое количество связей и соединен с определёнными соседними узлами. Примерами регулярных сетей являются решетки и кольца. Регулярные сети обладают высокой степенью предсказуемости, но

менее устойчивы к сбоям, чем сети со случайной или более сложной структурой.

— Масштабно-инвариантные сети (Scale-free Networks). В масштабно-инвариантны сетях распределение степеней узлов подчиняется степенному закону (power law). Это означает, что в сети существует небольшое количество узлов с очень большим количеством связей (так называемые «хабы» (hubs)), и большое количество узлов с малым количеством связей. Масштабно-инвариантные сети часто встречаются в реальном мире, например, в социальных сетях, интернете, биологических системах. Примером модели scale-free сети является модель Барабаши-Альберт (Barabasi—Albert model).

— Small-world сети (сети "малого мира"). Сети "малого мира" характеризуются тем, что средняя длина пути между любыми двумя узлами в сети относительно мала, несмотря на большой размер сети. Кроме того, данные сети обладают высоким коэффициентом кластеризации, что означает, что соседи узла, как правило, также связаны между собой. Примером модели small-world сети является модель Уоттса-Строгаца (Watts—Strogatz model).

Устойчивость сети (network robustness) — это способность сети сохранять свои основные функциональные характеристики при воздействии различных деструктивных факторов, таких как удаление узлов или рёбер. Устойчивость сети является комплексным понятием, зависящим от множества факторов, включая структуру сети, тип воздействия и критерии оценки [8], [9].

— Размер крупнейшей компоненты связности (Giant Component Size, GCS). Размер наибольшей связанной подсети после удаления определенного количества узлов или рёбер. Уменьшение размера крупнейшей компоненты связности свидетельствует о разрушении связности сети. GCS обычно выражается в процентах от общего количества узлов в сети.

— Средняя длина пути (Average Path Length, APL). Среднее расстояние между всеми парами узлов, принадлежащих к крупнейшей компоненте связности. Увеличение средней длины пути свидетельствует о снижении эффективности передачи информации в сети.

— Коэффициент связности (Connectivity Coefficient, CC). Мера связности сети, определяемая как отношение количества существующих рёбер к

максимально возможному количеству рёбер. Уменьшение коэффициента связности свидетельствует о разрушении связности сети.

— Эффективность передачи информации (Efficiency of Information Transfer, E). Оценивает способность сети передавать информацию между узлами. Эффективность может быть измерена различными способами, например, как обратная величина средней длины пути или как отношение количества достижимых узлов к общему количеству узлов.

Под атакой на сеть понимается преднамеренное или случайное воздействие, приводящее к удалению узлов или рёбер из сети. Обычно атаки на сеть меняют её топологию и заполняют сеть большим количеством однотипных пакетов для того, чтобы восстановление изначального состояния маршрутов было невозможно. Под случайными атаками, рассматриваемым в данной работе, подразумеваются кибератаки, при которых злоумышленник не выбирает конкретную цель, а атакует узлы сети или системы в произвольном порядке, без учёта их характеристик и положения в сети. [10]

Математические модели предоставляют формальный аппарат для анализа устойчивости сетей, основанный на теории графов, теории вероятностей и других математических дисциплинах.

Во втором разделе представлен процесс разработки модели устойчивости сети к случайным атакам, в том числе выбор инструментов, архитектура приложения и реализация моделей сетей.

Для разработки модели для исследования устойчивости для заданного графа требуется:

1. Определить функцию устойчивости $R(p) : [0, 1] \to [0, 1]$, где p — доля сохранившихся узлов;
2. Найти критическое значение p_c, при котором происходит фазовый переход (разрушение гигантской компоненты);
3. Сравнить $R(p)$ для рассматриваемых моделей сетей.

Основные критерии устойчивости:

1. Интегральная устойчивость: $R_{int} = \int_0^1 S(p)dp$ [11], где $S(p)$ — относительный размер гигантской компоненты.
2. Критический порог: $p_c = inf p : S(p) < 0.01$.
3. Локальная чувствительность: $\partial S/\partial p$ [11] в окрестности p_c.

Дополнительные метрики:

— Изменение среднего пути $L(p)$;
— Динамика коэффициента кластеризации $C(p)$;
— Распределение размеров компонент.

Целью разработки имитационной модели является исследование устойчивости различных типов сетей к случайным атакам, которые заключаются в последовательном удалении узлов. Для этого было разработано приложение на языке программирования Python 3.10 с использованием библиотек NetworkX, Matplotlib, Tkinter и Random.

При разработке приложения использовался объекто-ориентированный подход и элементы паттерна Model-View-Controller [12]. Model-View-Controlle (MVC) — это архитектурный паттерн проектирования, который позволяет разделять приложение на три основных компонента [13]: Модель (Model), отвечающий за данные приложения, Представление (View), отвечающий за отображение данных пользователю и получение данных от модели, и Контроллер (Controller), обрабатывающий пользовательский ввод и управляющий взаимодействием модели и представления.

В разработанном приложении реализованы четыре фундаментальные модели сетей: модель Эрдёша-Реньи, модель Барабаши-Альберт, модель Уоттса-Строгаца и конфигурационная сеть. Каждый тип сетей обладает своими уникальными свойствами и поведением при случайных атаках, что показано в Таблице 1:

Таблица 1 – Сравнительный анализ моделей сетей

Параметр	**Случайная сеть**	**Масштабно-инвариантная сеть**	**Сеть "малого мира"**	**Конфигурационная сеть**
Распределение степеней	Пуассоновское	Степенное	Промеж-точное	Заданное вручную
Наличие хабов	Нет	Ярко выражены	Слабо выражены	Зависит от распределения

Кластерный коэффициент	Низкий	Переменный	Высокий	Низкий
Средний путь	Короткий	Очень короткий	Короткий	Короткий
Устойчивость к атакам	Средняя	Высокая*	Высокая	Зависит от $p(k)$: если степенное — как у масштабно-инвариантных сетей, если Пуассоновское — как у случайной

Разработанный в приложении алгоритм случайных атак реализует последовательное строго случайное удаление узлов из сети. При удалении очередного узла каждый раз перерасчитываются значения гигантской компоненты, среднего кратчайшего пути и проверяется достижение критического порога.

Взаимодействие пользователя с приложением происходит через визуальный интерфейс, позволяющий выбирать модель генерируемой сети, её размер и прочие необходимые для генерации параметры, а также удалять узлы по одиночке вручную, или же запускать алгоритм автоматической случайной атаки до полной деградации сети.

В третьем разделе представлен анализ результатов моделирования и оценка устойчивости сети, включающие в себя итоговую таблицу.

Первым этапом исследования была генерация сетей различных топологий. Вторым этапом было моделирование случайных атак путём последовательного удаления строго случайных узлов. После каждого удаления сеть обновляется, и анализируются её ключевые параметры, что отображается на

графиках. При достижении критического порога процесс останавливается, а в графиках отображается значение критического порога устойчивости исследуемой сети.

Для количественного анализа устойчивости сетей к случайным атакам в данном эксперименте используются три ключевых критерия:

1. Размер гигантской компоненты. Гигантская компоненты — это наибольшая связная подгруппа узлов, в которой существует путь между любой парой узлов, её размер является основным индикатором глобальной связности сети [14].
2. Средняя длина кратчайшего пути. Средняя длина кратчайшего пути — это среднее число шагов, необходимых для перемещения между случайно выбранными узлами [15].
3. Критический порог. Критический порог f_c — это доля удалённых узлов, при которой сеть теряет свои ключевые свойства [16].

Так как визуализация играет ключевую роль в исследовании устойчивости сетей к случайным атакам, то для приложения был разработан простой пользовательский интерфейс, позволяющий визуализировать сети в виде графов и графики динамики деградации сети.

Результаты экспериментов в случайных сетях Эрдёша-Реньи показали, что сеть демонстрирует плавное возрастание среднего кратчайшего пути при доле удалённых узлов менее, чем $f \approx 0.8$, размер гигантской компоненты также уменьшается постепенно. При достижении же доли удалённых узлов $f > 0.8$ значение среднего кратчайшего пути резко возрастаетдо бесконечности.

Масштабно-инвариантные сети проявили иное поведение. В них отсутствует чёткий критический порог, а сама сеть проявляет стабильные свойства.

Устойчивость сетей типа "малый мир" средняя. В ходе экспериментов они демонстрировали поведение, промежуточное между случайными и масштабно-инвариантными сетями.

Конфигурационные же сети обладают различными сценариями устойчивости в зависимости от распределения степеней. В ходе экспериментов они проявили свойства близкие к масштабно-инвариантным сетям.

В результате проведённых экспериментов была получена следующая сравнительная Таблица 2:

Таблица 2 – Сравнение критериев для разных типов сетей

Параметр	**Случайная сеть**	**Scale-free сеть**	**Small-world сеть** ($p = 0.1$)	**Конфигурационная сеть** ($p = 0.1$)
Критический порог f_c	0.75	> 0.9	0.85	0.2
Скорость фрагментации	Высокая	Низкая	Средняя	Высокая
Рост средней длины пути	Резкий	Плавный	Умеренный	Резкий
Сохранение кластеров	Нет	Да	Частично	Нет

ЗАКЛЮЧЕНИЕ

В данной дипломной работе было проведено комплексное исследование устойчивости выбранных для исследования моделей сетей к случайным атакам. Основной целью работы являлась разработка приложения для анализа поведения сетей при воздействии случайных удалений узлов, а также сравнение устойчивости сетей с разными топологическими характеристиками. В ходе исследования были успешно решены поставленные задачи.

Были рассмотрены такие модели сетей, как Эрдёша-Реньи, Барабаши-Альберта, Уоттса-Строгаца и конфигурационные сети. Было разработано приложение на языке Python 3.10, позволяющее генерировать выбранные для исследования модели сети и оценивать их устойчивость с использованием метрик, таких как размер гигантской компоненты, средняя длина кратчайшего пути и критический порог разрушения. Приложение обеспечивает наглядную визуализацию, что упрощает анализ данных.

В будущем разработанное приложение может быть расширено добавлением дополнительных моделей сетей, учёта динамических изменений в сети, механизмов восстановления после атак и т.д.

Полученные результаты позволяют не только лучше понять механизмы устойчивости, но и предложить практические рекомендации для создания более надёжных сетевых систем.

Основные источники информации:

1 S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley and S. Havlin. Catastrophic cascade of failures in interdependent networks. Nature, 464: 08932, 2010.

2 Yoann Vandoorselaere, Laurent Oudot, “Prelude, an Hybrid Open Source Intrusion Detection System”, URL’: http://www.prelude-ids.org/ (Дата обращения: 19.03.2025)

3 A. Mounji, Languages and Tools for Rule-Based Distributed Intrusion Detection, PhD Thesis, Computer Science Institute, University of Namur, Belgium, Sept 1997.

4 Yates, David M. (1997). Turing’s Legacy: A History of Computing at the National Physical Laboratory 1945-1995. National Museum of Science and Industry. pp. 132–4. ISBN 978-0-901805-94-2.

5 Бройдо В. Л., Ильина О. П. Архитектура ЭВМ и систем: Учебник для вузов. 2-е изд.. — СРБ: "Издательский дом Питер 2021. — С. 21. — 720

с. — ISBN 978-5-4461-9983-9

6 Stephen McQuerry (29 May 2008). "Chapter 1: Building a Simple Network". Network World. Archived from the original on 8 July 2013. Retrieved 16 May 2012

7 Grant, T. J., ed. (2014). Network Topology in Command and Control. Advances in Information Security, Privacy, and Ethics. IGI Global. pp. xvii, 228, 250. ISBN 9781466660595

8 Albert-Laszlo Barabasi Network Science Network Robustness, 10, 58. 2024

9 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. — Спб.: Питер, 2010. — 944 с.: ил.

10 Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей учеб. пособие. — М.: ИД "ФОРУМ": ИНФА-М, 2008. — 416 с.: ил. — (Профессиональное образование). ISBN 978-5-8199-0331-5 (ИД "ФОРУМ") ISBN 978-5-16-003132-3 (ИНФРА-М)

11 Ivan Kryven. General expression for the component size distribution in infinite configuration networks // Physical Review E. — 2017. — Май (т. 95, вып. 5).

12 The Python Standard Library URL: https://docs.python.org/3/library/index.html (Дата обращения: 18.04.2025)

13 Trygve M. H. Reenskaug/MVC Архивировано 25 апреля 2018 года. XEROX PARC 1978-79

14 Molloy, M. and Reed, B. (1995) Random Structures and Algorithms 6, 161–180.

15 Barabasi, Albert-Laszlo; Zoltan N., Oltvai. (2004). "Network biology: understanding the cell's functional organization". Nature Reviews Genetics. 5 (2): 101–113.

16 Руслан Смелянский. Программно-конфигурируемые сети. Открытые системы. СУБД, №9. Открытые системы (20 ноября 2012). Архивировано 27 января 2013 года. URL: https://www.webcitation.org/6DyOwYRyU?url=http://www.osp.ru/os/2012/09 /13032491/ (Дата обращения: 03.06.2025)