Анализ сетевой устойчивости и оптимизация обмена данными в банковских системах

Н.Б. Лазарева, Д.С. Ефимов
Тихоокеанский государственный университет, Хабаровск

Аннотация: В статье представлен анализ сетевой устойчивости современных банковских систем с точки зрения теории графов. Использование графовых моделей позволяет эффективно описывать сложные сетевые структуры, выявлять узкие места и предсказывать поведение системы при сбоях или атаках. Предложены алгоритмы на основе теории графов, такие, как Алгоритм Дейкстры, для обеспечения минимального времени обработки транзакций и повышения надежности системы. Проведен сравнительный анализ различных методов оптимизации через моделирование на абстрактных графах и реальных данных банковской сети. В результате исследования предложены решения для защиты банковской системы, а также улучшения ее связности и отказоустойчивости.
Ключевые слова: Банковская система, теория графов, алгоритм Дейкстры, блокчейн, транзакции, кибератака, анализ сетевой устойчивости, банковская инфраструктура, кибербезопасность, DDoS-атака.

Современные банковские системы представляют собой сложные сети, взаимодействующие через обширные каналы обмена данными. Устойчивость этих сетей к сбоям и кибератакам является критическим фактором для обеспечения бесперебойной работы и защиты конфиденциальной информации. Применяя теорию графов для анализа сетевой устойчивости банковских систем, создадим макет стратегии противодействия кибератакам на основе полученных результатов. Особое внимание нужно уделить оптимизации обмена данными между элементами банковских сетей: филиалами, серверами, процессинговыми центрами и другими узлами. Это повысит надежность, а также скорость произведения транзакций.

На данный момент, в связи с недавними событиями в нашей стране, участились случаи серьезных кибератак и мошеннических действий во всех регионах. Любой обычный гражданин, зависимый от материальных средств, увидевший брешь в банковской системе, обязательно воспользуется в нужный момент данным ему преимуществом. По статистике за II квартал 2024 года количество кибератак в России выросло в два раза, по сравнению с

I кварталом. На рис.1 представлена прогнозируемая статистка кибератак к 2030 году.

Рис. 1. – Прогнозируемая статистика

Банковскую систему можно представить в виде графа G=(V, E) (рис.2), где: V – множество вершин, представляющих различные компоненты системы (филиалы, серверы, платежные системы и т.д.); E – множество ребер, представляющих каналы связи между компонентами. Вес каждого ребра может отражать пропускную способность канала, задержку передачи данных или уровень безопасности [1]. Различные типы кибератак могут быть смоделированы как удаление вершин или ребер из графа. Например, DDoS-атака на сервер может быть представлена удалением соответствующей вершины, а атака на канал связи – удалением ребра [2]. Таким образом, можно проанализировать, эффективность банковсой системы, ее защищенность, а также быстродействие.

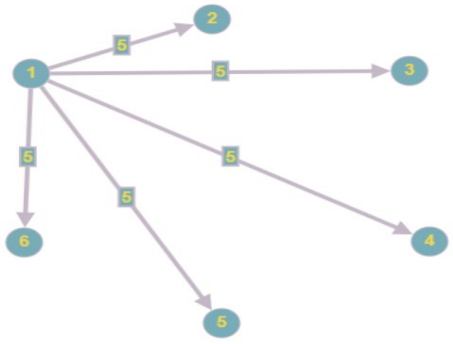

Рис. 2. – Пример графа банковской системы

Для оценки устойчивости банковской сети можно использовать различные метрики теории графов [3]:

1. Связность: измеряет степень взаимосвязанности компонентов сети. Высокая связность указывает на большую устойчивость к сбоям.
2. Диаметр: определяет максимальное расстояние между любыми двумя вершинами в графе. Меньший диаметр означает более быстрый обмен данными.
3. Центральность: позволяет определить наиболее важные узлы в сети, которые являются критическими для ее функционирования. Например, центральность показывает, сколько кратчайших путей проходит через данную вершину.
4. Доминирующие множества: минимальное множество вершин, которые контролируют всю сеть. Идентификация доминирующих множеств позволяет определить критически важные компоненты, требующие повышенной защиты.

Теория графов также позволяет оптимизировать обмен данными в банковской сети. Алгоритмы поиска кратчайших путей могут быть использованы для определения оптимальных маршрутов передачи данных, минимизирующих задержки и обеспечивающих максимальную пропускную способность. Алгоритмы потоковых сетей позволяют определить максимальный поток данных между двумя компонентами сети.

Алгоритм Дейкстры [4] — распространённый алгоритм нахождения кратчайших путей в графе с неотрицательными весами ребер от одной стартовой вершины до всех остальных (рис.3). Алгоритм работает пошагово [5] — на каждом шаге «посещается» одна вершина и уменьшается метка. Алгоритм Дейкстры начинается с подготовки графа и определения начальных условий и продолжается с итеративного обновления информации о кратчайших путях.

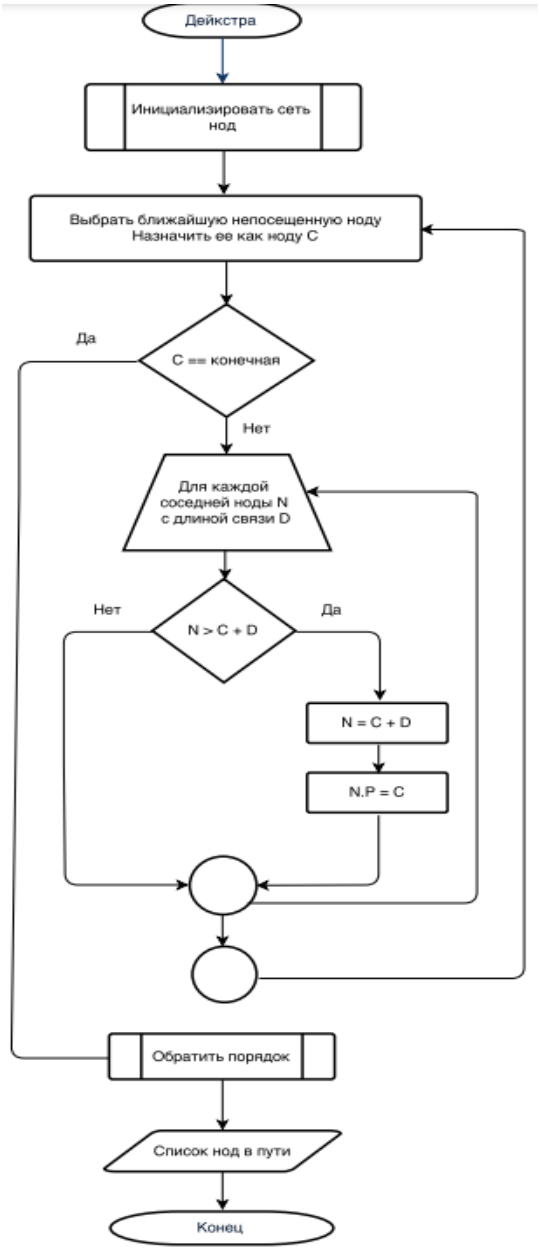

Рис. 3. – Блок-схема Алгоритм Дейкстры

1. Начальной вершине (допустим *a*) присваивается метка равная 0. Это значит, что путь от вершины *a* до самой себя имеет длину 0. Метки для всех остальных вершин устанавливаются как бесконечные. Это символизирует, что начальные расстояния от вершины *a* до них еще не определены.

2. Все вершины изначально считаются непосещёнными. Это будет означать, что они не участвовали в построении уже известных кратчайших путей.

3. Основной цикл алгоритма Дейкстры заключается в следующих действиях, которые повторяются до тех пор, пока не будут обработаны все вершины: из всех непосещённых вершин выбирается вершина (допустим *u*) с наименьшей меткой. Таким образом минимальная метка определяет путь с малейшей стоимостью.

4. Рассматриваются все возможные маршруты, в которых вершина *u* является предпоследним пунктом. Вершины, в которые ведут рёбра из *u*, называется соседями этой вершины. Для каждого соседа вершины *u*, кроме отмеченных как посещённые, рассматривается новая длина пути, равная сумме значений текущей метки *u* и длины ребра, соединяющего *u* с этим соседом. Если полученное значение длины меньше значения метки соседа, заменяется значение метки полученным значением длины. Рассмотрев всех соседей, помечается вершина *u*, как посещённая и шаг алгоритма повторяется.

5. Вершина *u* помечается как посещённая, что больше не требует ее рассмотрения в следующих итерациях.

6. Если множество всех вершин помечено как посещённое, алгоритм прекращает свою работу. Это означает, что рассмотрены все возможные оптимальные пути.

Проведя этап оптимизации сети, следующим шагом становится рассмотрение кибератак. Существует множество видов кибератак, и их классификация может варьироваться в зависимости от используемых критериев. Однако, можно выделить несколько основных категорий [6]:

1) По цели нападения. Такие атаки, как:

1. Атаки на инфраструктуру: нацелены на повреждение или выведение из строя компьютерных систем и сетей. Сюда входят DDoS-атаки (распределённые атаки типа "отказ в обслуживании"), атаки на серверы, атаки на маршрутизаторы и другие сетевые устройства.

2. Атаки на данные: нацелены на кражу, модификацию или уничтожение данных. Сюда относятся фишинг, атаки с использованием вредоносного ПО (вирусы, трояны, черви), атаки на базы данных [7].

3. Атаки на приложения: нацелены на уязвимости в программном обеспечении. Это могут быть эксплойты, SQL-инъекции (SQLi – уязвимость, которая позволяет атакующему использовать фрагмент вредоносного кода на языке структурированных запросов (SQL) для манипулирования базой данных и получения доступа к потенциально ценной информации), XSS (англ. Cross-Site Scripting — «межсайтовый скриптинг» — довольно распространенная уязвимость, которую можно обнаружить на множестве веб-приложений.).

4. Атаки на пользователей: нацелены на обман или манипулирование пользователями для получения доступа к их учетным данным или информации. Сюда относятся фишинг, социальная инженерия, атаки с использованием вредоносных ссылок.

2) По методу нападения. Включают:

1. Атаки с использованием вредоносного ПО (Malware): вирусы, трояны, черви, ransomware (программы-вымогатели), spyware (программы-шпионы), adware (рекламное ПО).

2. Атаки на основе уязвимостей: эксплуатация уязвимостей в программном обеспечении или операционных системах.

3. Социальная инженерия: манипулирование людьми для получения доступа к информации или системам.

4. Фишинг: получение конфиденциальной информации (пароли, номера кредитных карт) под видом легитимной организации.

5. DDoS-атаки: перегрузка сервера или сети запросами с множества источников, что приводит к отказу в обслуживании.

6. SQL-инъекции: ввод вредоносного кода в поля ввода веб-приложений для получения доступа к базе данных.

7. Man-in-the-middle (MITM) атаки: перехват коммуникации между двумя сторонами.

3) По масштабу атаки делятся на:

1. Целевые атаки: нацелены на конкретную организацию или человека.

2. Массовые атаки: нацелены на большое количество жертв.

Это лишь некоторые из основных видов кибератак (рис.4). В реальности существует множество вариаций и комбинаций этих методов, и киберпреступники постоянно разрабатывают новые способы атак.

Рис. 4. – Виды киберугроз

Для защиты от кибератак используется следующая структура безопасности [8] (рис.5):

1. Усиление защиты критически важных компонентов: идентификация узлов с высокой центральностью позволяет сфокусировать усилия по обеспечению безопасности на наиболее важных компонентах системы.

2. Резервирование каналов связи: разработка резервных маршрутов передачи данных позволяет обеспечить непрерывность работы системы в случае атаки на основной канал.

3. Разработка систем обнаружения вторжений: мониторинг сетевой активности позволяет своевременно обнаружить и предотвратить кибератаки.

4. Разработка стратегий восстановления после атак: разработка планов восстановления позволяет минимизировать последствия кибер-атак и быстро восстановить работоспособность системы.

Рис. 5. – Структура кибербезопасности

Для улучшения безопасности данных в банковской сфере можно использовать новые технологий (например, blockchain, искусственный интеллект (ИИ)). Это повлияет на обмен данными и сетевую устойчивость банковской системы безопасности. Внедрение технологий ИИ и машинного обучения в системы мониторинга позволяет улучшить обнаружение угроз. Эти технологии способны анализировать большие объемы данных и выявлять паттерны поведения, указывающие на атаки, что значительно повышает эффективность мониторинга. Blockchain (англ. blockchain, изначально block chain — цепь из блоков) — выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих какую-либо информацию [9]. Связь между блоками обеспечивается не только нумерацией, но и тем, что каждый блок содержит свою собственную хеш-сумму и хеш-сумму предыдущего блока. Изменение

любой информации в блоке изменит его хеш-сумму. Чтобы соответствовать правилам построения цепочки, изменения хеш-суммы нужно будет записать в следующий блок, что вызовет изменения уже его собственной хеш-суммы. При этом предыдущие блоки не затрагиваются. Если изменяемый блок последний в цепочке, то внесение изменений может не потребовать существенных усилий. Но, если после изменяемого блока уже сформировано продолжение, то изменение может оказаться крайне трудоёмким процессом. Дело в том, что обычно копии цепочек блоков хранятся на множестве разных компьютеров независимо друг от друга (рис.6).

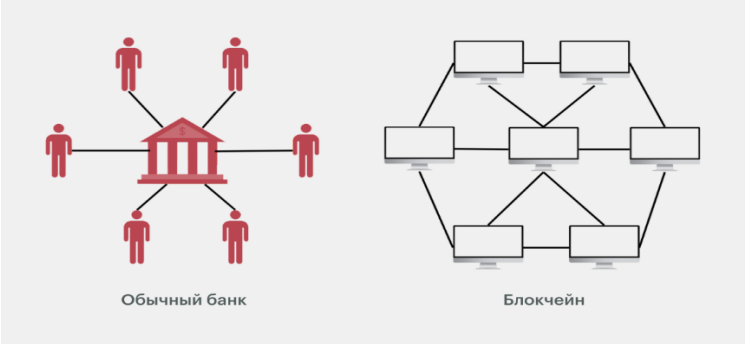

Рис. 6. – Отличие Blockchain от обычной банковской системы

Структура блокчейна напоминает графы [10]. Блокчейн можно представить как ориентированный граф (ОГ): блоки — это узлы, а связи между блоками (хэш-ссылки на предыдущие блоки) — это ориентированные ребра. В классических блокчейнах, подобных Bitcoin, это приводит к линейной цепочке блоков — линейному ОГ. Некоторые блокчейны, например IOTA, используют более сложную структуру — ориентированный ациклический граф (ОАГ, или DAG) (рис.7). В DAG(ОАГ) каждый блок может ссылаться на несколько предшествующих блоков (транзакций); отсутствуют циклы: невозможно вернуться к уже пройденной точке, обеспечивая строгое упорядочение транзакций во времени; параллельная обработка транзакций становится возможной благодаря этой структуре.

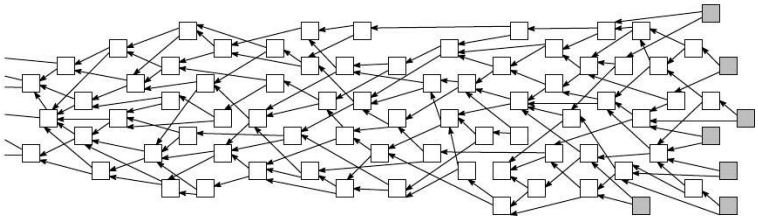

Рис. 7. – DAG(OAГ) криптовалюты IOTA

Однако внедрение блокчейна в банковскую систему — это сложный и многогранный процесс, который сулит как значительные преимущества, так и определённые вызовы. Преимущества включают:

1. Повышение эффективности: блокчейн может автоматизировать многие банковские процессы, такие как обработка платежей, подтверждение транзакций и ведение учета, что значительно сокращает время и затраты. Например, международные переводы могут стать быстрее и дешевле.

2. Повышение безопасности: децентрализованная природа блокчейна делает его более устойчивым к мошенничеству и киберпреступлениям [11]. Криптографическая защита данных обеспечивает высокую степень конфиденциальности.

3. Повышение прозрачности: все транзакции записываются в общедоступный (или контролируемый) реестр, что повышает прозрачность и подотчетность банковских операций. Это может помочь в борьбе с отмыванием денег и финансированием терроризма.

4. Уменьшение рисков: блокчейн может снизить риски, связанные с человеческим фактором, такими как ошибки и мошенничество со стороны сотрудников.

5. Улучшение взаимодействия: блокчейн может упростить взаимодействие между банками и другими финансовыми учреждениями, а также между банками и клиентами.

Внедрение блокчейна в банковскую систему также сопряжено с некоторыми трудностями:

1. Регуляторные вопросы: отсутствие четкой нормативно-правовой базы для блокчейна создает неопределенность и препятствует его широкому внедрению.
2. Масштабируемость: некоторые блокчейн-платформы имеют ограниченную масштабируемость, что может затруднить обработку большого объема транзакций в банковской системе.
3. Интеграция с существующими системами: интеграция блокчейна с существующими банковскими системами может быть сложной и дорогостоящей.
4. Безопасность: хотя блокчейн сам по себе безопасен, уязвимости могут существовать в приложениях и инфраструктуре, использующих блокчейн.
5. Отсутствие стандартов: отсутствие общепринятых стандартов для блокчейна в банковской сфере затрудняет взаимодействие между различными системами.

В настоящее время многие банки экспериментируют с блокчейном, используя его для отдельных процессов, таких как обработка платежей или управление активами. Полное внедрение блокчейна в банковскую систему — это долгосрочная перспектива, которая потребует решения многих технических и регуляторных проблем. Однако, потенциал блокчейна для трансформации банковской отрасли огромен.

Таким образом, применение теории графов для анализа сетевой устойчивости и оптимизации обмена данными в банковских системах является эффективным инструментом для обеспечения безопасности и бесперебойной работы. Идентификация слабых мест и разработка соответствующих стратегий противодействия кибератакам позволяют значительно снизить риски и обеспечить надежное функционирование банковской инфраструктуры. Дальнейшие исследования могут быть

направлены на разработку более сложных моделей, учитывающих динамические изменения в сети и более разнообразные типы кибератак [12].

Литература

1. Ковган Н.М. Компьютерные сети. Минск: РИПО, 2019. 179 с.
2. Мирзоев М.С. Основы математической обработки информации. Москва: Прометей, 2018. 318 с.
3. Уилсон Р. Введение в теорию графов. Диалектика, 2019. 240 с.
4. Титаев А.А. Промышленные сети. Екатеринбург: Уральский федеральный университет, 2020. 124 с.
5. Олифер Н., Олифер В. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2021. 1008 с.
6. Erickson J. Hacking: The Art of Exploitation. No Starch Press, 2008. P. 488.
7. Clarke Richard A., Knake Robert K. The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. Penguin Press, 2019. P. 352.
8. Dimaggio J. The Art of Cyberwarfare: An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime. No Starch Press, 2022. P. 272.
9. Генкин А.С., Михеев А. Блокчейн: как это работает и что ждёт нас завтра. Москва: Альпина Паблишер, 2018. 587 с.
10. Дрешер Д. Основы Блокчейна. Москва: ДМК Пресс, 2018. 312 с.
11. Пахаев Х.Х., Айгумов Т.Г., Абдулмукминова Ф.М. Роль технологии блокчейн в реализации кибербезопасности // Инженерный вестник Дона, 2022, №10. URL: ivdon.ru/magazine/archive/n10y2022/7958/.
12. Чибинев Н.Н., Ляшенко Н.В. Кибератака как новый вид чрезвычайных ситуаций // Инженерный вестник Дона, 2024, №7. URL: ivdon.ru/magazine/archive/n7y2024/9323/.

References

1. Kovgan N.M. Komp'juternye seti [Computer networks]. Minsk: RIPO, 2019. 179 p.

2. Mirzoev M.S. Osnovy matematicheskoj obrabotki informacii [Fundamentals of mathematical information processing]. Moskva: Prometej, 2018. 318 p.

3. Uilson R. Vvedenie v teoriju grafov [Introduction to graph theory]. Dialektika, 2019. 240 p.

4. Titaev A.A. Promyshlennye seti [Industrial networks]. Ekaterinburg: Ural'skij federal'nyj universitet, 2020. 124 p.

5. Olifer N., Olifer V. Komp'juternye seti. Principy, tehnologii, protokoly [Computer networks. Principles, technologies, protocols]. SPb.: Piter, 2021. 1008 p.

6. Erickson J. Hacking: The Art of Exploitation. No Starch Press, 2008. P. 488.

7. Clarke Richard A., Knake Robert K. The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. Penguin Press, 2019. P. 352.

8. Dimaggio J. The Art of Cyberwarfare: An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime. No Starch Press, 2022. P. 272.

9. Genkin A.S., Miheev A. Blokchejn: kak jeto rabotaet i chto zhdjot nas zavtra [Blockein: how it works and what awaits us tomorrow]. Moskva: Al'pina Pablisher, 2018. 587 p.

10. Dresher D. Osnovy Blokchejna [Fundamentals of Blockchain]. Moskva: DMK Press, 2018. 312 p.

11. Pahaev H.H., Ajgumov T.G., Abdulmukminova F.M. Inzhenernyj vestnik Dona, 2022, №10 URL: ivdon.ru/magazine/archive/n10y2022/7958/.

12. Chibinev N.N., Ljashenko N.V. Inzhenernyj vestnik Dona, 2024, №7. URL: ivdon.ru/magazine/archive/n7y2024/9323/.

Дата поступления: 18.12.2024

Дата публикации: 27.01.2025