КВАНТОВО-ФРАКТАЛЬНЫЙ МЕТОД ИДЕНТИФИКАЦИИ ЦИФРОВЫХ СЛЕДОВ
QUANTUM-FRACTAL DIGITAL TRACE IDENTIFICATION METHOD

Погребинская Мария Николаевна,
студентка Московского государственного
технического университета им. Н. Э. Баумана (МГТУ им. Баумана).
Pogrebinskaya Maria Nikolaevna,
student of the Bauman Moscow State Technical University (BMSTU).

Работа подготовлена с использованием системы КонсультантПлюс.

Аннотация. В условиях стремительного развития цифровых технологий и усложнения методов киберпреступной деятельности возникает потребность в новых подходах к выявлению, анализу и атрибуции цифровых следов. В статье рассматривается квантово-фрактальный метод идентификации цифровых следов, объединяющий принципы фрактального анализа и квантовых вычислений. Основу методики составляет использование фрактальной размерности и других статистических показателей самоподобия, позволяющих фиксировать скрытые закономерности в цифровой активности злоумышленника. Ключевым преимуществом подхода становится устойчивость к фрагментарности и изменчивости цифровых следов, а также возможность восполнения утраченной информации за счет структурной самоподобности. Использование квантовых алгоритмов обеспечит экспоненциальное ускорение обработки и сопоставления фрактальных шаблонов поведения, что критически важно при работе с большими объемами данных. Предложенная модель позволит формировать уникальные фрактальные профили киберпреступников, повышая точность и оперативность атрибуции, обеспечит превентивный мониторинг угроз в распределенных информационных системах.

Ключевые слова: киберпреступления, цифровые следы, фрактальный анализ, квантовые вычисления, фрактальная размерность, алгоритм Гровера, цифровая криминалистика, идентификация, атрибуция, квантово-фрактальный метод, самоподобие, большие данные, цифровая безопасность, DDoS-атаки, экспертные системы.

Summary. With the rapid development of digital technologies and the increasing complexity of cybercrime methods, there is a need for new approaches to identifying, analyzing, and attributing digital footprints. The article discusses a quantum-fractal method for identifying digital footprints that combines the principles of fractal analysis and quantum computing. The methodology is based on the use of fractal dimension and other statistical indicators of self-similarity, which make it possible to detect hidden patterns in the digital activity of an attacker. The key advantage of the approach is its resistance to fragmentation and variability of digital footprints, as well as the ability to replenish lost information through

structural self-similarity. The use of quantum algorithms will provide exponential acceleration of processing and matching fractal patterns of behavior, which is critically important when working with large amounts of data. The proposed model will allow the formation of unique fractal profiles of cybercriminals, increasing the accuracy and efficiency of attribution, and will provide preventive threat monitoring in distributed information systems.

Keywords: cybercrime, digital footprints, fractal analysis, quantum computing, fractal dimension, Grover algorithm, digital forensics, identification, attribution, quantum fractal method, self-similarity, big data, digital security, DDoS attacks, expert systems.

В условиях тотальной цифровизации киберпреступники оставляют все более сложные цифровые следы, обладающие распределенным, фрагментарным и обезличенным характером. Они лишены традиционных физических признаков (запах, форма), могут постоянно меняться, удаляться или подменяться, поэтому быстрое и надежное их обнаружение является нерешенной проблемой. Традиционные методы криминалистики, адаптированные к электронным доказательствам, полезны для анализа лог-файлов, скриншотов и данных мобильных устройств, однако уже в ближайшем будущем они не справятся с ростом объемов информации и изощренностью атак. В сложившейся ситуации актуальность приобретает квантово-фрактальный метод идентификации цифровых следов для работы с непрерывно обновляющимися данными.

Фрактальный анализ, лежащий в основе предлагаемого подхода, опирается на концепцию самоподобия и дробной размерности. Многие явления и процессы в цифровой среде обнаруживают статистическую самоподобность на разных масштабах времени. Для их количественной оценки может быть использована фрактальная размерность, в том числе размерность Минковского (метод коробочного счета). Известно, что при DDoS-атаках значение фрактальной размерности резко возрастает, позволяя оперативно идентифицировать аномалии. В квантово-фрактальной модели каждый новый фрагмент цифрового следа дополняет единую фрактальную структуру поведения и при этом меняет метрики (фрактальную размерность,

спектр фрактальной меры и т.д.). Если сохранение самоподобных характеристик указывает на непрерывность одного и того же сценария или на участие одного и того же субъекта, то резкие отклонения свидетельствуют либо о попытках подменить данные, либо о вмешательстве третьих лиц.

Наряду с фрактальным анализом эта методика задействует и квантовые вычисления, позволяющие экспоненциально ускорять поиск заданных шаблонов и пересчет фрактальных параметров. Квантовый поиск (алгоритм Гровера) теоретически способен мгновенно проверять совпадение или несовпадение паттернов, что крайне важно в ситуациях, когда сетевые логи или базы данных правоохранительных органов достигают колоссальных размеров. При поступлении новой информации квантовый компьютер оперативно корректирует «фрактальный портрет» злоумышленника, сохраняя целостную картину его действий. Кроме того, квантовая модель дает возможность учитывать корреляции между разрозненными фрагментами цифровых следов благодаря механизму квантовой запутанности. Фрактальная же компонента обеспечивает дополнительную устойчивость к неполноте исходных данных: если часть криминалистически значимой информации утеряна, самоподобная структура оставшихся данных позволяет восполнить пробелы в общей динамике событий.

Практическое применение квантово-фрактальной идентификации охватывает широкий спектр задач. Прежде всего, метод упрощает обнаружение киберпреступлений в распределенных системах. В средах с колоссальными потоками данных фрактальные показатели помогают быстро отслеживать аномальные события и связывать их воедино, если атака затронула несколько серверов. Так, при многоуровневом вторжении квантово-фрактальный анализ выявит общую фрактальную «подпись», характерную для одного организатора, что заметно ускорит атрибуцию. Кроме того, специалисты получат возможность проводить экспресс-оценку цифровых носителей непосредственно на месте происшествия: квантовый процессор выделяет ключевые «фрактальные» маркеры, которые фиксируются в виде

цифровых идентификаторов, привязанных к конкретным координатам (времени и месту). Эти идентификаторы служат своего рода контрольными суммами, позволяя при повторном анализе быстро определить, не была ли часть сведений утрачена или умышленно искажена.

Важным преимуществом квантово-фрактального метода становится повышенная точность атрибуции. Поскольку каждое действие в киберпространстве может обладать малозаментыми статистическими закономерностями, злоумышленник непреднамеренно оставляет специфический «фрактальный след». Квантовые алгоритмы могут получить возможность сопоставлять такой след с уже известными шаблонами, хранящимися в базах правоохранительных органов, что ускорит идентификацию подозреваемых. Теоретически возможно формировать базы данных не только с IP-адресами и хеш-суммами, но и с фрактальными профилями преступников. Благодаря этому при возникновении нового инцидента система автоматически сравнивает цифровой след с ранее зафиксированными образцами, оперативно предлагая круг лиц, потенциально причастных к атаке.

Описанный метод открывает возможности для превентивного мониторинга национальных сегментов сети, позволяет выявлять скоординированные кибератаки, организованные международными группами; он также может быть полезен при расследовании преступлений в сфере экономической деятельности, где трансакции разбросаны по множеству узлов; фрактальные модели помогают связать разрозненные действия в целостный узор схемы. Потенциально метод может лечь в основу экспертных систем: анализируя обновляющиеся фрактальные метрики, алгоритмы смогут советовать, какие серверы следует немедленно проверить, какие документы необходимо истребовать в первую очередь.

Таким образом, новизна квантово-фрактального подхода состоит, во-первых, в синергетическом слиянии квантовых и фрактальных методов, а во-вторых – в ориентации на непрерывно изменяющиеся цифровые следы,

которые трудно зафиксировать и систематизировать привычными способами. Практическая значимость подтверждается известными результатами фрактального анализа аномалий (например, всплеск фрактальной размерности при DDoS-атаках), а также активным развитием квантовых вычислений, повышающих производительность обработки больших данных. Разумеется, метод требует дальнейшей конкретизации, доработки и экспериментальной проверки: необходимо протестировать прототип квантовой системы мониторинга, интегрированной с инфраструктурой больших данных правоохранительных органов, а также сформировать правовую базу для признания результатов такого анализа доказательством. Однако уже сейчас ясно, что в перспективе квантово-фрактальная идентификация существенно расширяет инструментарий криминалистики, повышая шансы на быструю и точную атрибуцию противоправной деятельности в киберпространстве.

Список литературы:

1. Закиян А. А. Цифровые следы в криминалистике / А. А. Закиян // Молодой ученый. – 2023. – №23 (470). – С. 326–328.
2. Bulavas V. Fractal dimensionality of network traffic as a feature for intrusion detection // Proceedings of the International Conference on Security & Defence (ICSD). – 2020. – P. 45–47.
3. Цифровой след // Большая российская энциклопедия [электронный ресурс]. – URL: https://bigenc.ru/c/tsifrovoi-sled-0e7ff5 (дата обращения: 01.03.2025).
4. The Impact of Quantum Computing on Digital Forensics and Cybersecurity [Электронный ресурс] // BM Coder, 2023. – URL: https://www.bmcoder.com/the-impact-of-quantum-computing-on-digital-forensics-and-cybersecurity (дата обращения: 01.03.2025).
5. What is the Impact of Quantum Computing on Digital Forensics? – The Complete Guide [Электронный ресурс] // Web Asha, 2023. – URL: https://www.webasha.com/blog/what-is-the-impact-of-quantum-computing-on-digital-forensics (дата обращения: 01.03.2025).