Секция «LegalTech. Цифровая криминалистика»

Квантово-фрактальный метод идентификации цифровых следов

Научный руководитель – Яковлев Алексей Николаевич

Погребинская Мария Николаевна

Студент (специалист)

Московский государственный технический университет имени Н.Э. Баумана, Москва, Россия

E-mail: mashapogrebinskaya@yandex.ru

В условиях всепроникающей цифровизации киберпреступники оставляют все более сложные цифровые следы, обладающие распределенным, фрагментарным и обезличенным характером. В них не просматривается традиционных физических признаков [1], они 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 (далее – КФМИ) цифровых следов.

Фрактальный анализ, лежащий в основе предлагаемого подхода, опирается на концепцию самоподобия и дробной размерности. Многие явления и процессы в цифровой среде обнаруживают статистическое самоподобие в различных временных горизонтах [3; 1]. Для их количественной оценки может быть использована фрактальная размерность, в том числе размерность Минковского. Известно, что при DDoS-атаках значение фрактальной размерности резко возрастает, позволяя оперативно идентифицировать аномалии [2; 28]. В модели КФМИ 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.

Особенностью методики является комплексное применение фрактального анализа и квантовых вычислений, позволяющее экспоненциально ускорять поиск заданных шаблонов и пересчет фрактальных параметров [5]. Алгоритм Гровера позволяет быстро находить совпадения в массивных сетевых логах и базах данных правоохранительных органов, значительно ускоряя процесс анализа. 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 КФМИ упрощает обнаружение киберпреступлений в распределенных системах. В средах с колоссальными потоками данных фрактальные показатели помогают быстро отслеживать аномалии и связывать их воедино, если атака затронула несколько серверов. Так, при многоуровневом вторжении КФМИ выявит общую «подпись», характерную для одного организатора, что заметно ускорит атрибуцию. Кроме того, специалисты получат возможность проводить экспресс-оценку цифровых носителей на

месте происшествия: квантовый процессор выделяет ключевые «фрактальные» маркеры, которые фиксируются в виде 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 КФМИ станет повышенная точность атрибуции. Поскольку каждое действие в киберпространстве обладает малозаментыми статистическими закономерностями, злоумышленник непреднамеренно оставляет специфический «фрактальный след» [4]. Квантовые алгоритмы получат возможность сопоставлять такой след с 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 сравнит цифровой след с ранее зафиксированными образцами, предложит круг лиц, потенциально причастных к атаке.

КФМИ даст возможности для превентивного мониторинга национальных сегментов сети, позволяет выявлять скоординированные кибератаки, организованные международными группами; он также будет полезен при расследовании преступлений в сфере экономической деятельности, где трансакции разбросаны по множеству узлов. 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 КФМИ состоит, во-первых, в синергетической отдаче сочетания квантовых и фрактальных методов, а во-вторых – в ориентации на непрерывно изменяющиеся цифровые следы, которые трудно зафиксировать привычными способами. Разумеется, метод требует доработки и экспериментальной проверки: необходимо протестировать прототип квантовой системы мониторинга, интегрированной с инфраструктурой больших данных, сформировать правовую базу для признания результатов такого анализа доказательством. Однако уже сейчас ясно, что в перспективе КФМИ существенно расширит инструментарий криминалистики, повышая шансы на быструю и точную атрибуцию противоправной деятельности в киберпространстве.

Источники и литература

1) Закиян А. А. Цифровые следы в криминалистике / А. А. Закиян // Молодой ученый. – 2023. – №23 (470). – С. 326–328.

2) Перов Р. А., Лаута О. С., Крибель А. М., Федулов Ю. В. Метод выявления аномалий в сетевом трафике // Наукоемкие технологии в космических исследованиях Земли. 2022. №3. URL: https://cyberleninka.ru/article/n/metod-vyyavleniya-anomaliy-v-setevom-trafike (дата обращения: 01.03.2025).

3) 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.

4) Цифровой след // Большая российская энциклопедия [Электронный ресурс]. – URL: https://bigenc.ru/c/tsifrovoi-sled-0e7ff5 (дата обращения: 01.03.2025).

5) 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).