Научная статья
УДК 343.98
doi: 10.17223/15617793/514/27

Датацентризм как основа цифровой трансформации раскрытия, расследования и предупреждения преступлений

Александр Борисович Смушкин[1]

[1] *Саратовская государственная юридическая академия, Саратов, Россия, Skif32@yandex.ru*

Аннотация. Предлагается новая концепция датацентризма как одного из основных факторов цифровой трансформации раскрытия, расследования и предупреждения преступлений. Предполагается, что датацентризм должен включать: расширение круга используемой в расследовании информации, её источников, усложнение методов работы с информацией, увеличение скорости обработки информации, усиление надёжности и безопасности хранения и обработки информации электронного документооборота, а также уделение повышенного внимания аналитическим методам и расширение круга методов дистанционного сбора информации. Последовательно рассматриваются приведенные элементы и даются рекомендации по каждому из них.
Ключевые слова: датацентризм, цифровая трансформация расследования, распределенная информация, raid-массивы, сетевое профилирование, методы интеллектуальной разведки, интеллектуальный анализ данных, применение нейросетей, анализ больших данных

Источник финансирования: исследование выполнено за счет гранта Российского научного фонда № 24-28-00312, https://rscf.ru/project/24-28-00312/.

Для цитирования: Смушкин А.Б. Датацентризм как основа цифровой трансформации раскрытия, расследования и предупреждения преступлений // Вестник Томского государственного университета. 2025. № 514. С. 234–241. doi: 10.17223/15617793/514/27

Original article
doi: 10.17223/15617793/514/27

Datacentrism as the basis for the digital transformation of crime detection, investigation and prevention

Aleksandr B. Smushkin[1]

[1] *Saratov State Law Academy, Saratov, Russian Federation, skif32@ya.ru*

Abstract. The author proposes a new concept of datacentrism as one of the most important aspects and drivers of the digital transformation of crime detection, investigation and prevention. The article is based on the use of materialistic dialectics as a universal method, as well as general scientific methods such as analysis, synthesis, modeling, extrapolation, and others. The author includes in datacentrism: expanding the range of information used in the investigation, its sources; increasing the complexity of methods of working with information; increasing the speed of information processing; increasing the reliability and security of storing and processing information in electronic document management; paying increased attention to analytical methods and expanding the range of methods for remote information collection. The author consistently examines these elements and makes recommendations for each of them. As part of the expansion of the range of information used in the investigation, new types and forms of information are considered, as well as the need to activate new methods of searching for orienting and evidentiary information: methods of intellectual intelligence. It is stated that the specifics of working with certain types of distributed information and services for working with it (for example, peer-to-peer networks, Raid arrays, blockchain, other distributed registries, etc.), remote work with information, splitting an information object into small parts and finding parts from different people or on different hard drives (in Raid arrays) and so on require the development of special recommendations. The author highlights the need for new forms of information retrieval and defines the specifics of network profiling, OSINT, data mining, Big Data analysis, automation of information collection and research using neuromorphic technologies. The main directions of the implementation of data-centric methods and tools are: (1) building and estimating the probability of versions using automated technologies; (2) determining the priorities of the investigation; (3) identification of potential witnesses; (4) crime prevention. The conclusions indicate that: the application of the ideas of datacentrism in investigative activities for the detection, investigation and prevention of crimes can significantly increase the effectiveness of the investigation. This information acquires evidentiary value being confirmed by the results of investigative actions; the use of a platform concept organized according to a block-modular principle with different levels (circles) of access will ensure effective access to data for both managers and specific researchers, as well as analysts, technical specialists and other involved persons, while maintaining the restrictions provided for by law; a cloud-based form of information storage is suggested as optimal.

Keywords: datacentrism, digital transformation of investigations, distributed information, raid arrays, network profiling, intelligent intelligence methods, data mining, application of neural networks, big data analysis

Financial support: The research was supported by the Russian Science Foundation, Project No. 24-28-00312, https://rscf.ru/project/24-28-00312/

***For citation*:** Smushkin, A.B. (2025) Datacentrism as the basis for the digital transformation of crime detection, investigation and prevention. *Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal*. 514. pp. 234–241. (In Russian). doi: 10.17223/15617793/514/27

Четвёртая информационная революция, а также появление новых видов и форм информации приводят к насущной необходимости разработки методов, средств и технологий работы с информацией, а также, в некотором смысле, и парадигмы расследования – началу цифровой трансформации расследования.

Представляется, что в настоящее время основой цифровой трансформации раскрытия, расследования, предупреждения преступлений должен стать датацентризм, включающий расширение круга используемой в расследовании информации, её источников, усложнение методов работы с информацией, увеличение скорости обработки информации, усиление надёжности и безопасности хранения и обработки информации электронного документооборота, а также уделение повышенного внимания аналитическим методам и расширение круга методов дистанционного сбора информации.

Как отметили О.А. Зайцев и П.С. Пастухов, «технология аналитической работы следователя заключается в получении нового знания (выводной информации), обеспечивающего сложный процесс расследования, имеющий определенную логическую последовательность. Аналитический характер такого расследования состоит из взаимосвязанных рабочих операций, которые образуют технологический цикл отбора, группировки фактов о событиях, явлениях, процессах, где каждый факт обретает свое место и связан с предшествующими и последующими обстоятельствами в пространственно-временной и причинно-следственной зависимости причастных к преступлению лиц. Обобщение фактов, их научная обоснованная систематизация позволяют дать правильную оценку как всей совокупности фактов, так и каждого из них в отдельности» [1. С. 765].

С учётом расширившегося спектра электронной информации, сопровождающей жизнь каждого пользователя, можно говорить о том, что почти каждое действие человека оставляет следы в виртуальном киберпространстве.

О.Ю. Введенская в своей диссертации ввела достаточно интересную концепцию «криминалистическая ёмкость следа». Под криминалистической емкостью она понимает «способность объекта воспринимать, хранить и отражать объем информации о преступном деянии, в ходе совершения которого он был задействован, тем самым описывая совершенное преступление» [2. С. 127]. Как мы уже отмечали ранее, в рамках криминалистической деятельности эффективнее использовать категорию «криминалистическая информационная емкость объекта», которая отражает меру возможного нахождения потенциальной криминалистической значимой информации [3. С. 42].

Информационная ёмкость различных объектов и видов следов существенно отличается. Особенности максимально точного извлечения информации из материальных и идеальных следов достаточно подробно разработаны в криминалистике.

Виртуальным же (цифровым, электронным) следам особое внимание стало уделяться относительно недавно в масштабах развития науки криминалистики [4–8]. Криминалистическая информационная ёмкость виртуальных следов существенно выше традиционных. То есть и потенциальная возможность перевода криминалистической значимой потенциальной информации в актуальную доказательственную, по нашему мнению, выше иных видов.

Возможности использования в расследовании электронных устройств и информационных технологий приводят к актуализации разработок частных теорий, связанных с обнаружением, фиксацией, изъятием и исследованием виртуальных следов информационно-технологических устройств, а также использованием цифровых технологий в ходе расследования (цифровая криминалистика [9], электронно-цифровая криминалистика [10], киберкриминалистика [11], форензика [12] и т.д.).

В рамках данных частных теорий своё место получают также методы обнаружения, фиксации, изъятия и исследования новых видов и форм информации (распределённой информации, облачной информации, нейроморфных вычислений, дистанционных форм работы с информацией и т.д.).

Специфика направления работы с отдельными видами распределённой информации и сервисами работы с ней (например, пиринговыми сетями, Raid-массивами, блокчейном, иными распределёнными реестрами и т.д.), дистанционной, удаленной работы с информацией (т.е. фактически наличия «чистого», пустого компьютера-терминала, с которого производилась работа, при основном дистанционном сервере и возможность дистанционной модификации информации в новом месте), дробление информационного объекта на небольшие части и нахождение частей у разных людей либо на разных жёстких дисках (в Raid-массивах) и так далее требуют разработки особых рекомендаций, которыми должен руководствоваться следователь в ходе производства следственных действий. Во многом возникает необходимость использования и обработки новых источников информации и новых методов работы с ней. Этому будет способствовать реализация концепции датацентризма в расследовании. Современная криминалистика находится на пороге новых возможностей, открытых благодаря развитию технологий обработки данных и анализа информации.

В контексте цифровизации и глобализации феномен датацентризма становится неотъемлемой частью практик расследования и реальных кейсов уголовных дел, предоставляя возможность превращать массивы данных в ценную криминалистически значимую информацию. Это принципиально новый подход к организации процессов, в котором данные рассматриваются как первичный и наиболее ценный ресурс. Все оперативно-розыскные, следственные и экспертные мероприятия строятся вокруг сбора, стандартизации, интеграции, комплексного анализа и интерпретации данных из самых разнообразных источников. Датацентрическая криминалистика должна стремиться объединить всю полученную процессуальным и непроцессуальным путем информацию в единое информационное пространство, обогащая их данными из открытых и закрытых цифровых источников с целью установления в ходе анализа полученного информационного конструкта скрытых закономерностей, выявления неочевидных связей, построения предиктивных моделей поведения преступников и оптимизации процесса принятия решений.

Конечно, расширение спектра используемой информации в рамках парадигмы датацентризма не говорит о необходимости полного перехода на американские стандарты, в рамках которых в доказывании может использоваться любая информация, по которой может быть подтверждена «цепочка законных владений». Однако необходима активизация новых методов поиска ориентирующей и доказательственной информации: методов интеллектуальной разведки, таких как OSINT, Humint, Cybint, Geoint, Finint, Data mining и Data extracting, сетевое профилирование и т.д.

Использование методов сетевого профилирования в оперативно-розыскной и следственной практике в отдельных случаях имеет место уже сейчас. Так, достаточно часто профилируются педофилы, экстремисты и т.д. С точки зрения концепции датацентризма мы полагаем необходимым перманентный мониторинг сети Интернет для выявления специфических групп, каналов, объединяющих людей с характерными преступными наклонностями, с помощью нейросетевых технологий или разработанных алгоритмов (например, программного комплекса «Демон Лапласа», различных систем линейки Крибрум (Крибрум.Объекты, Крибрум. Публичный поиск и т.д.)). При этом мы настаиваем на необходимости производства мониторинга сети именно в доследственном режиме, поскольку именно в этот период злоумышленники могут проявлять меньшую осторожность и использование таких результатов максимально обеспечивает фактор внезапности. В случае выявления подобных лиц с помощью методов Osint и Cybint должна быть собрана информация о страницах в сети и иных информационных ресурсах, принадлежащих указанному пользователю и размещенных в открытом режиме. На основе активности лица в сети (частота публикаций, тематика сообщений, стиль общения, круг контактов, геолокация, используемые устройства) может быть сформирован цифровой профиль злоумышленника.

Значение будет иметь как общее исследование сетевых ресурсов, созданием или моделированием которых занимается объект, а также ресурсов, на которых он упоминается, так и его страницы в социальных сетях. При исследовании страницы социальной сети будут иметь значение фотографии (что изображено, фон, тип, цвет, тональность и т.д.); указание биографических данных; статус, выставленный пользователем; размещённые на странице видео и музыкальные произведения; лайки (новости, книги, видео и музыкальное ресурсы, заинтересовавшие и положительно отмеченные автором); круг друзей; группы; сообщества, в состав которых входит объект и т.д.

На точность сетевого профилирования могут влиять цель создания страницы, желание показаться более загадочным, более уверенным в себе человеком, приверженцем определенных взглядов либо сверстником круга, в который пытается войти человек, а также отражать идеальный образ, к которому стремится создающий страницу. Это может приводить к несоответствию сетевого профиля реальному человеку, дифференциации виртуальной и реальной личности человека.

Проводимые исследования возможны как в «живом» режиме специалистами-психологами, так и с помощью специально разработанных программ, в том числе и основанных на нейроморфных технологиях. В любом случае результат должен быть изучен, оценен и прокомментирован специалистом в заключении специалиста или в показаниях в ходе допроса специалиста. Полученные результаты должны обязательно учитываться при разработке тактических приемов последующих следственных и иных процессуальных действий. Конечно, данные сетевого профилирования не могут иметь прямого доказательственного значения, а могут лишь дополнять имеющуюся информацию, ориентировать следователя или оперативного сотрудника при выборе тактических приемов и комбинаций, а также последовательности, условий и времени проведения оперативных мероприятий и процессуальных действий. Однако их значение в современных условиях должно быть существенно повышено, становясь неотъемлемым элементом, сопровождающим расследование сложных, резонансных или многоэпизодных преступлений. Полученные данные могут также применяться для сужения круга подозреваемых, выявления новых эпизодов преступной деятельности, прогнозирования поведения и выбора тактики оперативно-розыскных мероприятий.

Сетевое профилирование – мощный инструмент, но его применение требует баланса между технологической эффективностью, законностью и этикой. Кроме того, результаты сетевого профилирования должны также сопоставляться с данными традиционного криминалистического профилирования. Для оценки качества сетевого профилирования также могут быть привлечены специалисты по анализу цифровых данных, лингвисты, психологи и IT-эксперты для комплексной оценки информации и повышения качества профилирования.

Методы интеллектуальной разведки, будучи изначально предназначенными для сбора информации невластными субъектами, в ходе расследования получают дополнительное развитие, обеспечиваясь правомочиями следователя и оперативного сотрудника. Так, методы Geoint могут реализовываться на базе соглашений следственного комитета РФ с Роскосмосом. Для получения снимков запрос направляется через Главное управление криминалистики (Криминалистический центр) Следственного комитета Российской Федерации в государственную корпорацию Роскосмос. Возможно также использование приложений, находящихся в открытом доступе, например Google Eartch. Несмотря на ретроспективность данных методов познания, научно-технический прогресс, увеличение спутниковой группировки и разрешающей способности установленного оборудования, скорости передачи данных и других факторов, есть основание предполагать возможность появления уже в ближайшее время новых тактических приемов, связанных с использованием дистанционного зондирования Земли в режиме реального времени.

Проблемы применения Osint и Cybint в отечественных условиях связаны, прежде всего, с ограничением доступа ко многим сетевым ресурсам не только регистрацией на сайте, но и вхождением в определенный круг (друзей, единомышленников и т.д.). Следователь (оперативный сотрудник) вынужден использовать либо открытые источники с применением методов OSINT, или направление запроса модератору ресурса, либо получение судебного разрешения на производство определенных ОРМ и последующим взаимодействием с провайдером. Для указанных целей в европейском законодательстве (например, Королевства Испания или ФРГ) используется концепция «служебного вируса» – программ взлома закрытых аккаунтов. Мы полагаем, что ограниченное конкретными условиями, под жестким судебным контролем и допустимое к производству только оперативно-техническими подразделениями ФСБ, подобное действие могло бы иметь существенный эффект и в России.

Как отмечают специалисты, «при поиске информации в интернете в ходе OSINT используются следующие основные элементы: поисковые машины (веб-браузеры), основные запросы пользователей и ключевые слова, гиперссылки интернет-страниц, базы данных, платные и бесплатные онлайн-сервисы, соцсети, люди (пользователи сети). В ходе сборе информации могут использоваться как открытые, так и конфиденциальные источники» [13. С. 13]. В рамках данного вида интеллектуальной разведки деятельность специалистов включает в себя поиск информации, процессы ее очистки, валидации, накопления данных, анализа и обработки информации. Существенно повысить эффективность аналитической работы можно за счет использования и учета не только технических, но и психологических особенностей участников, составления поведенческих профилей.

Применение методов пассивной интеллектуальной разведки (без взаимодействия с целью или ее окружением) сохраняет в тайне интерес следствия или оперативно-розыскных органов к конкретному лицу, что позволит в дальнейшем, собрав определенный объем информации, максимально использовать фактор внезапности при производстве следственных действий и ОРМ. Пассивно методы, например OSINT, могут применяться с использованием таких программных инструментов, как АПК «Виток-OSINT», Moltego, Shodan, Recon-ng, телеграмм-ботов, и других. Однако необходимо отметить огромный объем «информационного шума», который может вызвать сложности фильтрации.

Результаты применения OSINT в криминалистических целях могут быть использованы, например, для поиска свидетелей, проверки показаний, установления и проверки алиби (в том числе цифрового алиби), выдвижения версий о мотивах содеянного обнаружения в сети следов мошенничества, экстремизма, киберпреступлений. Кроме того, технологии OSINT могут использоваться и в рамках следственного действия. Так, К.Ю. Яковлева указывает на возможность использования подобных технологий в рамках обыска в местах нахождения электронной информации (электронного обыска). Причем, поскольку использоваться будут только открытые источники, применение его не будет требовать судебного санкционирования. К.Ю. Яковлева отмечает, что «сущность данного обыска места нахождения электронной информации с помощью технологии OSINT заключается в следующем: применение элементов указанной технологии выражается в установлении связи данных одного лица, то есть персональные и другие данные, которое само же лицо разместило на разных страницах сети “Интернет”. Такая связь является дополнительной частью достаточных данных для производства обыска (поиска) на нескольких страницах сети “Интернет”» [14. С. 133].

Кроме того, А.А. Бессонов говорит о возможности применения указанных технологий в следующих целях:

– установление людей и связей между ними, включая скрытые и удаленные данные, социальные сети;

– поиск различных объектов и событий по географическим координатам;

– мониторинг закрытых преступных сообществ, форумов и маркетплейсов Даркнета;

– анализ контента социальных сетей и веб-страниц;

– анализ операций с криптовалютами [15. С. 44].

HUMINT как метод интеллектуальной разведки, традиционно полагаясь на интервью и информаторов, теперь интегрируется с большими данными посредством оцифрованных отчетов и анализа с помощью NLP. Кроме того, сам HUMINT начинает переходить в формат сетевого общения. Это может быть понимание «контекста» цифровых взаимодействий, анализ мотивов, скрытых за публичными сообщениями, верификация цифровых данных через нецифровые каналы, понимание групповой динамики в сетевых сообществах. Нужно уметь вызывать доверие, располагать к себе, задавать правильные вопросы. Иногда достаточно просто грамотно «разговорить» человека в онлайн-чате,

чтобы получить ценную информацию. Используя данные о людях и их поведении, аналитики могут глубже понять мотивацию преступников, что, в свою очередь, помогает в разработке стратегий по их задержанию. HUMINT позволяет не только собирать информацию, но и анализировать её с точки зрения человеческих факторов.

Результаты применения методов интеллектуальной разведки в уголовном деле могут отражаться справками, «выгруженными» из определенных открытых баз, заключениями специалистов, ответами на запросы следователя провайдерами и модераторами о принадлежности сетевых ресурсов, справками специалиста о результатах применения определенных программ (например, по местонахождению устройства с определенным IP-адресом) и т.д. Эффективным будет использование результатов применения методов интеллектуальной разведки в дополнение к традиционным доказательствам, например для «триангуляции» данных.

Датамайнинг (data mining, DM), или интеллектуальный анализ данных, используется для выстраивания сложных корреляционных взаимосвязей в большом объёме информации. Зарубежные авторы подчеркивают эффективность интеллектуального анализа данных при расследовании преступлений [16–18]. Алгоритмы машинного обучения позволяют выявлять скрытые закономерности в поведении пользователей социальных сетей. Это может помочь в идентификации групп риска или потенциальных преступников.

Одной из самых распространённых систем анализа за рубежом является программное обеспечение «Palantir»[1] от компании Palantir Technologies, выполняющее функции сбора и анализа разнородных данных, генерации на их базе новых данных, прогнозов, оповещений, визуализации событийного ряда.

Как отметил П.С. Пастухов, «Data Mining в уголовно-процессуальной и криминалистической деятельности – это просев информации, добыча данных, извлечение данных, а также интеллектуальный анализ данных, т.е. “обнаружение знаний в базах данных” криминалистически значимой доказательственной информации. Одно из важнейших назначений методов Data Mining состоит в наглядном представлении результатов вычислений (визуализация), особенно с использованием геоинформационных систем. Такая визуализация, например, местонахождения подозреваемого, позволяет использовать наглядное доказательство по уголовным делам» [19. С. 54]. Интеграция различных источников информации – от онлайн-ресурсов до результатов анализа больших данных – может создать более полную картину преступного события или профиль ее участника. Методы Data Mining могут использоваться для группировки преступлений по признакам, выявления типичных сценариев и построения прогнозов относительно будущих преступных действий или поведения подозреваемых, восстановления хронологии событий, визуализации связей между фигурантами, определения иерархии преступных групп и доказывания занятия высшего положения в преступной иерархии (ст. 210.1 УПК РФ). Для максимальной эффективности методов DM необходимо аккумулировать в одном цифровом информационном массиве всю стекающуюся органам следствия и дознания информацию, как доказательственного, так и ориентирующего, справочного и иного характера. Вся потенциально криминалистически значимая информация должна быть аппаратно структурирована, обработана с последующей валидацией и интерпретацией специалистами с выделением актуальной криминалистически значимой информации.

Анализ больших данных становится тем самым «двигателем», который перемалывает сырую информацию, выявляет неочевидные связи, подтверждает или опровергает гипотезы, выдвинутые на этапе профилирования. Это позволяет не просто реагировать на уже совершенные преступления, но и работать на упреждение, выявляя потенциальные угрозы и преступные сообщества на ранних стадиях их формирования. Однако следует учитывать, что анализ даже только тех данных, которые находятся в открытом доступе, может привести к установлению информации, которая может носить конфиденциальный характер в силу отнесения к тайне личной жизни, коммерческой тайне, медицинской тайне, информации об усыновлении и т.д. Поэтому особое значение приобретает этичность получения и использования указанной информации, а также обеспечение ее безопасности.

Важнейшими аспектами датацентризма можно назвать также автоматизацию сбора информации, расширения поиска (использование скрытых закономерностей и паттернов), анализ больших данных, использование нейросетей и искусственного интеллекта, активную визуализацию данных (построение социальных графов и т.д.), взаимную интеграцию технологий.

Автоматизация процесса сбора, систематизации и даже, частично, оценки информации, может способствовать повышению всесторонности и объективности исследования информации, снижению коррупциогенных и просто субъективных факторов, повышению скорости обработки информации, повышению глубины и качества извлекаемой криминалистически релевантной информации, одновременно используя различные источники, в том числе и несистематизированной разноплановой информации. Во многом подобная автоматизация поможет избежать ошибок субъективного характера.

Кроме того, можно отметить перспективы использования методов комплексного анализа, при котором повышение эффективности достигается за счёт использования сильных сторон каждого члена команды.

Датацентричные методы должны быть интегрированы в структуру частных криминалистических методик с адаптированными алгоритмами их применения для разных видов преступлений.

Представляется, что основными направлениями воплощения датацентричных методов и средств должны стать:

1) построение и оценка вероятности версий с использованием автоматизированных технологий;

2) определение приоритетов расследования;

3) выявление потенциальных свидетелей;

4) предотвращение преступлений.

Среди преимуществ внедрения датацентричных подходов можно отметить: повышение эффективности и оперативности расследования; снижение ошибок субъективного характера; возникновение новых источников информации; гибкость и адаптивность, позволяющие быстро приспособиться, адаптировать методы анализа к новым условиям.

Во многом данные, полученные с использованием датацентрического подхода, позволят прогнозировать поведение тех же подозреваемых, например, с использованием предлагаемой нами концепции «цифровых двойников». Под цифровым двойником преступника мы понимаем цифровую виртуальную модель злоумышленника или преступной группы, отражающую его основные характеристики и дающие возможность на базе известной следствию информации предположить определенную, подлежащую установлению информацию, а также действия злоумышленников. Д.А. Свиридов указывает, что «на основании массива собранных цифровых следов современные алгоритмизированные системы имеют возможность, отсеивая информационный шум, создать так называемый пузырь фильтров – эксклюзивную версию виртуального пространства человека» [20. С. 262]. Фактически подобный пузырь фильтров может использоваться и при моделировании предлагаемого нами цифрового двойника преступника.

Применение датацентрического подхода может способствовать выявлению корреляционных связей между людьми, явлениями и событиями. При этом представляется, что новые методы и технологии только при комплексном применении могут дать синергетический эффект повышения эффективности расследования.

Конечно, датацентризм снижает классические тактические риски в следственных действиях, однако можно отметить наличие некоторых факторов риска самого датацентристского подхода. Кроме того, можно отметить и некоторые сложности и проблемы использования и датацентризма:

Во-первых, сложность и вопросы доступности технологий приводят к цифровому неравенству следственных органов регионов. Не секрет, что техническая оснащенность, например, Следственного комитета в Москве и на окраинах Саратовской области существенно отличается.

Во-вторых, получение и обработка больших массивов информации могут выявить ошибки алгоритмов, неверные паттерны получаемых данных.

В-третьих, безусловно, поднимаются вопросы о конфиденциальности информации, этичности её получения и обработки, так как можно отметить, что из информации, которую человек не имеет намерения скрывать, вполне могут быть сделаны выводы, которые человек не хотел бы делать публично известными и публично доступными. Тот же анализ больших данных часто характеризуется непрямой корреляцией исследуемой информации, выводов. Связаны между собой могут быть факторы, находящиеся полностью в разных плоскостях. Так, американский исследователь Сет Стивенс-Давидовиц обнаружил корреляцию запросов в Google с увеличением уровня безработицы. Причем, как это ни странно, максимально увеличиваются запросы, связанные не с трудоустройством и биржами труда, а именно запросы на порносайты «в связи с увеличивающимся количеством свободного времени и снижением уровня усталости» [21. С. 97].

В-четвертых, непрозрачность алгоритмов работы нейросетей может увеличить риски ошибок машинного обучения или программных алгоритмов, а также отразить предубеждение программистов.

В-пятых, важной проблемой могут стать сложности с интерпретацией и интеграцией данных. Следователи не обладают достаточным опытом для интерпретации полученных данных и использования в расследовании. Следует также отметить сложность обучения и подготовки специалистов в данной сфере. К сожалению, сейчас учебные курсы подготовки, связанные с изучением указанных выше средств и методов, крайне редко имеют место или практически отсутствуют в программах не только гражданских, но и ведомственных вузов систем МВД и СКР, не говоря уже о гражданских вузах. Поэтому представляется крайне необходимым дополнение учебных программ специалитета или дополнительного профессионального образования данными курсами. До действующих следователей спектр возможностей рассматриваемого подхода может быть доведён в рамках периодического повышения квалификации.

Важнейшей проблемой могут стать и киберугрозы – использование сетевых электронных инструментов в рамках датацентризма повышает опасность кибератак, утечек информации. Это характеризует насущную необходимость принятия дополнительных мер по защите информации.

Таким образом, применение идей датацентризма в следственной деятельности по раскрытию, расследованию и предупреждению преступлений может существенно повысить эффективность расследования путём максимизации перевода потенциальной криминалистической значимой информации в актуальную. Безусловно, эту информацию можно использовать прежде всего в ориентирующих целях. Однако она приобретает доказательное значение, будучи подтверждена результатами следственных действий, основанных на ней. Кроме того, заслуживает особого внимания предложение О.А. Зайцева о переходе с доказательств документов на доказательства данных [1. С. 766].

Важной задачей реализуемой в рамках датацентрической концепции расследования является обеспечение создания инфраструктуры, которая бы предусматривала эффективный доступ к данным как руководителей и конкретных исследователей, так и аналитиков, технических специалистов и иных задействованных лиц, при сохранении предусмотренных законом ограничений на распространение информации, связанной со следственной и иными видами тайны. Выходом из подобной ситуации видится использование платформенной концепции, организованной по блочно-модульному принципу с различными уровнями (кругами) доступа. Цифровые платформы фактически станут «нервной системой» датацентричной криминалистики.

Для обеспечения повышения безопасности и коллаборации различных правоохранительных структур в противодействии преступной деятельности можно определить облачную форму хранения информации. О необходимости перевода информации правоохранительных структур в облачную среду уже ранее поднимался вопрос на официальном уровне. Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 гг. и на перспективу до 2025 г., утвержденная распоряжением Правительства Российской Федерации от 01 ноября 2013 № 2036-р., в рамках приоритетных с точки зрения и информационной безопасности направлений исследований и разработок в области информационных технологий называет стимулирование циркуляции данных «облачных» сервисов внутри страны[2]. Применение облачных вычислительных платформ предусмотрено и Концепцией цифровой трансформации органов прокуратуры в виде перевода «информационных систем и информационных ресурсов органов прокуратуры в создаваемую государственную единую облачную платформу с обеспечением хранения и обработки в ней всей создаваемой информации»[3]. Облачная платформа даст возможность одновременной работы нескольких пользователей с одной информацией. При этом повышение безопасности обеспечивается дроблением единого информационного объекта на множество частей и размещением их на различных серверах. При этом взлом одного сервера даст доступ только к одному элементу объекта, который изолированно даже не сможет быть прочитан.

Примечания

[1] Palantir. URL: https://www.palantir.com/

[2] Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года утверждена распоряжением Правительства Российской Федерации от 01 ноября 2013 № 2036-р. // Собрание законодательства РФ. 18.11.2013. № 46. Ст. 5954.

[3] Приказ Генеральной прокуратуры РФ от 14 сентября 2017 г. № 627 «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года» // Информационно-правовой портал Гарант. URL: https://www.garant.ru/products/ ipo/prime/doc/71670972/ (дата обращения 02.07.2024).

Список источников

1. Зайцев О.А., Пастухов П.С. Формирование новой стратегии расследования преступлений в эпоху цифровой трансформации // Вестник Пермского университета. Юридические науки. 2019. Вып. 46. С. 752–777.
2. Введенская О.Ю. Особенности предварительного и первоначального этапов расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий : дис. … канд. юрид. наук. Краснодар, 2022. 200 с.
3. Вехов В.Б., Смушкин А.Б. Об информационной емкости криминалистических объектов // Сибирские уголовно-процессуальные и криминалистические чтения. 2023. № 2 (40). С. 39–48.
4. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации : дис. … д-ра юрид. наук. Воронеж, 2001. 387 с.
5. Милашев В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ : дис. … канд. юрид. наук. М., 2004. 208 с.
6. Краснова Л.Б. Компьютерные объекты в уголовном процессе и криминалистике : дис. … канд. юрид. наук. Воронеж, 2005. 202 с.
7. Лыткин Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности : дис. … канд. юрид. наук. М., 2007. 201 с.
8. Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе : дис. … канд. юрид. наук. Воронеж : Воронежский государственный университет, 2010. 198 с.
9. Цифровая криминалистика : учеб. для вузов / В.Б. Вехов [и др.] ; под редакцией В.Б. Вехова, С.В. Зуева. 2-е изд., перераб. и доп. М. : Юрайт, 2024. 490 с.
10. Смушкин А.Б. Концептуальные основы частной теории электронной цифровой криминалистики (частной теории собирания, исследования и использования электронной цифровой информации и информационно-технологических устройств) / под общ. ред. В.Б. Вехова. М. : РУСАЙНС, 2022. 222 с.
11. Островский О.А. Киберкриминалистика в цифровую эпоху: вызовы и перспективы развития // Юридическая гносеология. 2024. № 5. С. 106–114.
12. Федотов Н.Н. Форензика – компьютерная криминалистика. М., 2007. 360 с.
13. Агафонов Е.П. Особенности использования OSINT в раскрытии и расследовании преступлений // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений : сб. материалов конф., Воронеж, 28 мая 2023 г. Воронеж : Воронежский институт Министерства внутренних дел Российской Федерации, 2023. С. 13–18.
14. Яковлева К.Ю. Использование технологии OSINT в ходе обыска места нахождения электронной информации // Проблемы правовой и технической защиты информации. 2023. № 11. С. 131–136.
15. Бессонов А.А. Использование в раскрытии преступлений информации из открытых источников информации (OSINT) // Актуальные вопросы теории и практики оперативно-разыскной деятельности: Межведомственная научно-практическая конференция, 16 сентября 2022 г. : сб. науч. тр. М. : Московский университет МВД России имени В.Я. Кикотя, 2022. С. 40–45.
16. Keyvanpour M.R., Javideh M., Ebrahimi M.R. Detecting and investigating crime by means of data mining: a general crime matching framework // Procedia Computer Science. 2011. Vol. 3. P. 872–880.
17. Ozkan K. Managing data mining at digital crime investigation // Forensic Science International. 2004. Vol. 146, Supplement. P. S37–S38.
18. Deepa D. Shankar, Adresya Suresh Azhakath, Nesma Khalil, Sajeev J., Mahalakshmi T., Sheeba K. Data mining for cyber biosecurity risk management – A comprehensive review // Computers & Security. 2024. Vol. 137. Art. No. 103627.
19. Развитие информационных технологий в уголовном судопроизводстве: монография / под ред. С.В. Зуева. М. : Юрлитинформ, 2018. 248 с.
20. Свиридов Д. А. Цифровой след и его значение в практике расследования преступлений // Правовая культура в современном обществе : сб. науч. ст. VI Междунар. науч.-практ. конф., Могилев, 19 мая 2023 года. Могилев : Могилевский институт Министерства внутренних дел Республики Беларусь, 2023. С. 260–263.
21. Стивенс-Давидовиц Сет. Все лгут. Поисковики, Big data и Интернет знают о вас все / [пер. с англ. Л.И. Степановой]. М. : Эксмо, 2020. 480 с.

References

1. Zaytsev, O.A. & Pastukhov, P.S. (2019) Formirovanie novoy strategii rassledovaniya prestupleniy v epokhu tsifrovoy transformatsii [Formation of a New Strategy for Crime Investigation in the Era of Digital Transformation]. *Vestnik Permskogo universiteta. Yuridicheskie nauki*. 46. pp. 752–777.
2. Vvedenskaya, O.Yu. (2022) *Osobennosti predvaritel'nogo i pervonachal'nogo etapov rassledovaniya nezakonnogo sbyta narkoticheskikh sredstv s ispol'zovaniem informatsionno-telekommunikatsionnykh tekhnologiy* [Features of the Preliminary and Initial Stages of Investigating the Illegal Sale of Narcotic Drugs Using Information and Telecommunication Technologies]. Law Cand. Diss. Krasnodar.
3. Vekhov, V.B. & Smushkin, A.B. (2023) Ob informatsionnoy emkosti kriminalisticheskikh ob"ektov [On the Information Capacity of Forensic Objects]. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniya*. 2 (40). pp. 39–48.
4. Meshcheryakov, V.A. (2001) *Osnovy metodiki rassledovaniya prestupleniy v sfere komp'yuternoy informatsii* [Fundamentals of the Methodology for Investigating Crimes in the Sphere of Computer Information]. Law Dr. Diss. Voronezh.
5. Milashev, V.A. (2004) *Problemy taktiki poiska, fiksatsii i iz"yatiya sledov pri nepravomernom dostupe k komp'yuternoy informatsii v setyakh EVM* [Problems of Tactics for Searching, Fixing and Seizing Traces in Cases of Unauthorized Access to Computer Information in Computer Networks]. Law Cand. Diss. Moscow.
6. Krasnova, L.B. (2005) *Komp'yuternye ob"ekty v ugolovnom protsesse i kriminalistike* [Computer Objects in Criminal Procedure and Forensics]. Law Cand. Diss. Voronezh.
7. Lytkin, N.N. (2007) *Ispol'zovanie komp'yuterno-tekhnicheskikh sledov v rassledovanii prestupleniy protiv sobstvennosti* [The Use of Computer-Technical Traces in the Investigation of Crimes Against Property]. Law Cand. Diss. Moscow.
8. Agibalov, V.Yu. (2010) *Virtual'nye sledy v kriminalistike i ugolovnom protsesse* [Virtual Traces in Forensics and Criminal Procedure]. Law Cand. Diss. Voronezh: Voronezh State University.
9. Vekhov, V.B. & Zuev, S.V. (eds) (2024) *Tsifrovaya kriminalistika* [Digital Forensics]. 2nd edition. Moscow: Yurayt.
10. Smushkin, A.B. (2022) *Kontseptual'nye osnovy chastnoy teorii elektronnoy tsifrovoy kriminalistiki (chastnoy teorii sobiraniya, issledovaniya i ispol'zovaniya elektronnoy tsifrovoy informatsii i informatsionno-tekhnologicheskikh ustroystv)* [Conceptual Foundations of the Private Theory of Electronic Digital Forensics (Private Theory of Collecting, Researching and Using Electronic Digital Information and Information Technology Devices)]. Moscow: Rusayns.
11. Ostrovskiy, O.A. (2024) Kiberkriminalistika v tsifrovuyu epokhu: vyzovy i perspektivy razvitiya [Cyber Forensics in the Digital Age: Challenges and Development Prospects]. *Yuridicheskaya gnoseologiya*. 5. pp. 106–114.
12. Fedotov, N.N. (2007) *Forensika – komp'yuternaya kriminalistika* [Forensics – Computer Crime Investigation]. Moscow.
13. Agafonov, E.P. (2023)[Features of Using OSINT in Crime Detection and Investigation]. *Prestupnost' v SNG: problemy preduprezhdeniya i raskrytiya prestupleniy* [Crime in the CIS: Problems of Crime Prevention and Detection]. Conference Proceedings. Voronezh. 28 May 2023. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation. pp. 13–18. (In Russian).
14. Yakovleva, K.Yu. (2023) Ispol'zovanie tekhnologii OSINT v khode obyska mesta nakhozhdeniya elektronnoy informatsii [The Use of OSINT Technology During the Search of the Location of Electronic Information]. *Problemy pravovoy i tekhnicheskoy zashchity informatsii*. 11. pp. 131–136.
15. Bessonov, A.A. (2022) [The Use of Open Source Intelligence (OSINT) in Crime Detection]. *Aktual'nye voprosy teorii i praktiki operativno-rozysknoy deyatel'nosti* [Current Issues in the Theory and Practice of Operational-Search Activity]. Proceedings of the Interdepartmental Conference. 16 September 2022. Moscow: Moscow University of the Ministry of Internal Affairs of Russia. pp. 40–45. (In Russian).
16. Keyvanpour, M.R., Javideh, M. & Ebrahimi, M.R. (2011) Detecting and investigating crime by means of data mining: a general crime matching framework. *Procedia Computer Science*. 3. pp. 872–880.
17. Ozkan, K. (2004) Managing data mining at digital crime investigation. *Forensic Science International*. 146 (Supplement). pp. S37–S38.
18. Shankar, D.D. et al. (2024) Data mining for cyber biosecurity risk management – A comprehensive review. *Computers & Security*. 137. Art. No. 103627.
19. Zuev, S.V. (ed.) (2018) *Razvitie informatsionnykh tekhnologiy v ugolovnom sudoproizvodstve* [Development of Information Technologies in Criminal Proceedings]. Moscow: Yurlitinform.
20. Sviridov, D.A. (2023) [The Digital Footprint and Its Significance in Crime Investigation Practice]. *Pravovaya kul'tura v sovremennom obshchestve* [Legal Culture in Modern Society]. Proceedingsof the VI International Conference. Mogilev. 19 May 2023. Mogilev: Mogilev Institute of the Ministry of Internal Affairs of the Republic of Belarus. pp. 260–263. (In Russian).
21. Stephens-Davidowitz, S. (2020) *Vse lgut. Poiskoviki, Big data i Internet znayut o vas vse* [Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are]. Translated from English by L.I. Stepanova. Moscow: Eksmo.

Информация об авторе:
Смушкин А.Б. – канд. юрид. наук, ведущий научный сотрудник проектного офиса научных программ и исследований, доцент кафедры криминалистики Саратовской государственной юридической академии (Саратов, Россия). E-mail: Skif32@yandex.ru

Автор заявляет об отсутствии конфликта интересов.

Information about the author:
A.B. Smushkin, Cand. Sci. (Law), leading research fellow, associate professor, Saratov State Law Academy (Saratov, Russian Federation). E-mail: skif32@ya.ru

The author declares no conflicts of interests.

Статья поступила в редакцию 03.04.2025;
одобрена после рецензирования 12.05.2025; принята к публикации 30.05.2025.

The article was submitted 03.04.2025;
approved after reviewing 12.05.2025; accepted for publication 30.05.2025.