ПРОИЗВОДСТВА ДОПРОСА ПО УГОЛОВНЫМ ДЕЛАМ О КИБЕРПРЕСТУПЛЕНИЯХ

Сабырбаева А.Б. -
доцент Академии МВД Республики Узбекистан,
доктор философии по юридическим наукам (PhD), доцент

Расследование киберпреступлений обладает высокой спецификой. Как справедливо указывает Д.М. Берова, следствие неизбежно сталкивается с огромными объемами цифровых данных (исчисляемых терабайтами), для анализа которых требуются «особые технологии и средства их обработки» и «определенные модели анализа» [1]. К этой технической специфике следует добавить и критический «временной фактор»: любое промедление позволяет преступникам уничтожить или изменить цифровые доказательства, что особенно актуально при работе с изменчивыми крипто-активами.

Критическое осмысление правоприменительной практики выявляет фундаментальную проблему: традиционный процессуальный инструментарий отстает от технологической динамики расследуемых деяний. Существующая процедура выемки и осмотра электронных носителей не учитывает летучесть оперативной памяти устройств и риск дистанционного уничтожения данных. Представляется обоснованным внедрение в первоначальный этап расследования обязательной процедуры криптографического хэширования изымаемых цифровых массивов непосредственно на месте производства следственного действия. Только математически подтвержденная неизменность хэш-суммы способна гарантировать процессуальную чистоту цифрового доказательства и исключить доводы стороны защиты о возможной компрометации данных до момента их экспертного исследования.

Хотя предварительное расследование преступлений, совершенных в киберпространстве, направлено на решение традиционных задач УПК (установление обстоятельств, сбор доказательств, изобличение виновных), в данной категории дел, как отмечают Н.А. Марочкин и Е.Н. Асташкина, этот процесс является «сложным, трудоёмким и ресурсозатратным» [2]. Следователю приходится обрабатывать огромные массивы информации (зачастую сотни гигабайт с одного устройства). Некоторые ученые, как О.А. Зайцев и П.С. Пастухов, разграничивают доказывание на «поиск» (на стадии предварительного следствия) и «убеждение» (на стадии суда) [3]. На наш взгляд, термин «убеждение» в контексте суда звучит не совсем корректно. Исходя из принципа непосредственности исследования доказательств, суд является независимым участником доказывания; он не нуждается в «убеждении» стороной обвинения, а обязан самостоятельно исследовать все представленные доказательства и обосновывать приговор только на них.

В ходе предварительного расследования по преступлениям, совершенным в киберпространстве, ключевое значение имеет четкое определение последовательности первоначальных этапов (как процессуальных, так и следственных). Этот первоначальный этап логически делится на несколько этапов. Во-первых, проводятся «стандартные» процессуальные действия: допрос потерпевшего; допросы «дропов» (в статусе свидетелей или подозреваемых, в зависимости от их осведомленности); привлечение лица в качестве подозреваемого и обеспечение участия защитника с последующим допросом. Во-вторых, проводится комплекс технических и специфических мероприятий: направляются запросы на крипто-биржи; производится обыск устройств с последующим вынесением постановления о признании изъятых электронных данных цифровыми доказательствами. Сюда же относится и сбор сетевых данных, включающий: выемку регистрационных данных о соединениях (трафике) и доступе в Интернет; направление запросов к хостинг-провайдерам (для получения сведений об IP-адресах, доменах, серверах и их владельцах); запросы в электронные платежные системы (о статусе идентификации пользователя и подключении карт); а также запросы в представительства социальных сетей и почтовых сервисов (например, mail.ru, rambler) для оказания содействия следствию.

Заявляя о необходимости направления запросов на криптовалютные биржи и к хостинг-провайдерам, следует открыто признать наличие острой проблемы — юрисдикционного барьера. Большинство ключевых платформ зарегистрированы в офшорных зонах, не имеющих с нашим государством договоров о взаимной правовой помощи. Использование стандартных каналов международного сотрудничества занимает долгие месяцы, за которые похищенные активы проходят десятки циклов микширования. В связи с этим возникает объективная необходимость лэгализации процедур прямого (экстерриториального) электронного взаимодействия следователя с комплаенс-подразделениями зарубежных платформ, минуя громоздкие бюрократические институты.

Одним из центральных следственных действий остается допрос. По замечанию М.В. Жижиной и Д.В. Завьяловой, именно он предоставляет следователю ту ориентирующую информацию, которая необходима для проверки имеющихся следственных версий [4]. Специфика допроса по киберпреступлениям напрямую продиктована цифровой природой следов и высокой компетенцией фигурантов. Следователь обязан детально разбирать технические логи, метаданные и способы анонимизации (VPN, Tor). Поскольку подозреваемые часто выстраивают защиту на сложном техническом жаргоне, списывая свои действия на системные ошибки или автоматизированные процессы, требуется оперативное взаимодействие с IT-специалистами.

Специфика допроса по преступлениям, совершенным в киберпространстве, обусловлена цифровой природой доказательств и часто высокой технической компетенцией участников событий. Это требует учета следующих особенностей:

- *необходимость детального разбора технических данных.* Следователь должен уметь работать с логами, временными метками, IP-адресами, метаданными и другими цифровыми следами. В процессе допроса важно задавать вопросы, касающиеся конкретных технических аспектов – какие программы или инструменты использовались для доступа к системам, каким образом осуществлялась анонимизация (например, через VPN, Tor или прокси-серверы), и каким образом организовывалась цепочка операций, позволяющая скрыть истинное происхождение атаки.

- *высокий уровень профессиональных знаний у подозреваемых,* что может приводить к использованию сложного технического жаргона и аргументации, затрудняющей выявление противоречий. Следователю необходимо либо обладать базовыми знаниями в области цифровой криминалистики, либо оперативно привлекать специалистов для интерпретации терминологии и оценки достоверности заявлений. Подозреваемые могут пытаться ссылаться на автоматизированные процессы или ошибки в системах как на оправдание своих действий, поэтому требуется сосредоточенное выяснение последовательности действий с опорой на объективно зафиксированные цифровые данные;

- *необходимость оперативного взаимодействия со специалистами в сфере IT-технологий.* Использование результатов технического анализа в реальном времени позволяет не только подтвердить или опровергнуть показания подозреваемого, но и выявить попытки манипуляций с цифровыми доказательствами. Такой подход требует организации следственных действий, на которых специалист может пояснить сложные технические моменты, а следователь – задать уточняющие вопросы, что существенно повышает качество и точность получаемой информации;

- *проверка временной последовательности событий*. Цифровые доказательства зачастую содержат точные временные метки, что позволяет сопоставлять показания подозреваемого с хронологией атаки. Следует задавать вопросы, направленные на выяснение, где и каким образом происходили конкретные операции, и как подозреваемый объясняет возможные временные расхождения, особенно если он пытается переложить ответственность на сторонние воздействия или автоматизированные системы;

- *детальный разбор методов маскировки и фальсификации электронных данных.* Преступники часто используют шифрование, стэганографию и другие технологии для сокрытия следов своих действий. Допрос в таком случае должен включать вопросы,

направленные на выяснение используемых технологий и инструментов, а также на проверку соответствия заявляемых методов фактическим цифровым следам. Подозреваемый может утверждать, что его система была взломана извне или что, использованные инструменты были доступны в свободном доступе, поэтому важно детально разобрать все технические нюансы и установить факт личного участия.

Наиболее распространенным видом допроса по этой категории дел является допрос потерпевшего, тактика которого выстраивается в зависимости от типа преступления и личности допрашиваемого. Ряд ученых указывают на необходимость криминалистической типологизации жертв. Так, А.А. Рукосуев предлагает классифицировать их в зависимости от готовности сотрудничать и добросовестности (например, активные/неактивные или добросовестные/недобросовестные жертвы) [5]. Более глубокий психологический подход предлагает Р.Л. Ахмедшин, разработавший типовые модели допрашиваемых на основе акцентуаций характера (гипертим, шизоид, эпилептоид и др.). По мнению автора, использование таких моделей позволяет следователю «более рационально осмыслить» имеющуюся тактическую информацию [6].

Анализ практики производства допроса потерпевших показывает, что его эффективность существенно снижается под воздействием ряда объективных и субъективных факторов. К субъективным относится тяжелое психоэмоциональное состояние жертвы (шок, состояние фрустрации, стыд за собственную доверчивость). Данный фактор особенно ярко проявляется в случаях, сопряженных с мошенническим оформлением на граждан крупных онлайн-кредитов, где до 49% потерпевших на первоначальном этапе не способны дать ясные и последовательные показания. К объективным факторам следует отнести специфику личности потерпевшего: возрастной критерий (например, при реализации схемы «Алло, мама», где жертвами преимущественно становятся лица старше 60 лет) и критически низкий уровень цифровой грамотности. Последнее обстоятельство блокирует возможность получения полных показаний о сугубо технических деталях совершенного деяния (сущности вредоносных ссылок, алгоритмах ввода кодов авторизации, названиях установленных программ удаленного доступа).

Преодоление указанных барьеров требует от лица, производящего расследование, адаптации классических приемов допроса. В условиях выраженного стресса и чувства вины за добровольную передачу конфиденциальных данных злоумышленникам традиционный вопросно-ответный формат оказывается малопродуктивным. В подобных ситуациях следственная практика диктует необходимость применения элементов когнитивного интервью. Эта методика позволяет без жесткого давления последовательно восстановить в памяти потерпевшего мельчайшие детали события: от фоновой обстановки в момент поступления звонка до точной хронологии манипуляций с мобильным устройством.

Учитывая, что жертва зачастую физически не способна воспроизвести техническую терминологию, допрос целесообразно проводить в неразрывной связи с процессуальным осмотром принадлежащих ей электронных носителей информации (смартфонов, планшетных компьютеров). Тактика следственного действия в этом случае сводится к совместному изучению сохранившихся цифровых следов: истории интернет-браузера, лог-файлов в мессенджерах, банковских push-уведомлений и SMS-сообщений с кодами подтверждения. При этом следователю надлежит формулировать уточняющие вопросы предельно ясно, избэгая излишнего технического усложнения речи, чтобы не спровоцировать у допрашиваемого защитную реакцию или отказ от дачи показаний из-за непонимания сути происходящего.

С процессуальной и криминалистической точек зрения показания потерпевшего по делам анализируемой категории выступают не только самостоятельным источником доказательств, но и первичным тактическим «путеводителем» для дальнейшего поиска электронных следов. Максимально точная фиксация времени поступления звонка, перехода по фишинговой ссылке или несанкционированного списания средств, достигнутая в ходе детализированного допроса, формирует документальную основу для оперативного

направления запросов в кредитные организации, провайдерам связи и владельцам интернет-сервисов. Именно поэтому такой допрос должен производиться незамедлительно, до наступления процесса естественного забывания деталей жертвой или автоматического уничтожения цифровых следов алгоритмами вредоносного программного обеспечения.

ЛИТЕРАТУРЫ:

1. Берова Дж.М. Расследование киберпреступлений // Пробелы в российском законодательстве. 2018. №2. URL: https://cyberleninka.ru/article/n/rassledovanie-kiberprestupleniy
2. Марочкин Н.А., Асташкина Е.Н. Алгоритмизация – эффективный метод оптимизации расследования преступлений // Известия Алтайского государственного университета. - №2. – 2001. – С. 45
3. Зайцев О.А., Пастухов П.С. Формирование новой стратегии расследования преступлений в эпоху цифровой трансформации // Вестник Пермского университета. Юридические науки. 2019. Вып. 46. С. 752777. DOI: 10.17072/1995-4190-2019-46-752-777
4. Жижина М.В., Завьялова Д.В. Расследование преступлений в сфере компьютерной информации в Российской Федерации и зарубежных странах: монография. Москва: Проспект, 2023.149 с.
5. Рукосуев А.А. Тактика производства следственных действий при расследовании киберпреступлений. Научный аспект №6. 2024. – Право. https://na-journal.ru/6-2024-pravo/13337-taktika-proizvodstva-sledstvennyh-deistvii-pri-rassledovanii-kiberprestuplenii
6. Ахмедшин Р.Л. Тактика коммуникативных следственных действий / науч. ред. Н.Т. Ведерников. – Томск: Издательский Дом ТГУ, 2014. – 50 с.

РЕЗЮМЕ:

Специфика цифровых следов требует адаптации классических следственных действий. В статье рассматриваются проблемы тактики производства допроса по делам о киберпреступлениях.

Ключевые слова: производство допроса, киберпреступления, тактика следственных действий

RESUME:

The specific nature of digital traces requires the adaptation of classical investigative actions. The article examines the tactical problems of conducting interrogations in cybercrime cases.

Keywords: conducting interrogation, cybercrimes, investigative tactics.

REZYUME:

Raqamli izlarning o‘ziga xosligi klassik tergov harakatlarini moslashtirishni talab qiladi. Maqolada kiberjinoyatlar bo‘yicha so‘roq qilish taktikasining muammolari ko‘rib chiqiladi.

Kalit so‘zlar: so‘roq o‘tkazish, kiberjinoyatlar, tergov harakatlari taktikasi.