ПОДОЛЬНЫЙ Р. Н., ПОДОЛЬНАЯ Н. Н.

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ПРИМЕНЕНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Аннотация. В настоящее время цифровые технологии применяются в ходе совершения преступлений, затрудняя восприятие в событиях и фактах признаков, указывающих на их криминальную сущность. Практика расследования преступлений, совершенных с применением цифровых технологий, сталкивается с проблемой понимания субъектами уголовного судопроизводства обстоятельств их совершения. Одним из средств преодоления трудностей выявления и расследования этих преступлений является привлечение специальных знаний в сфере цифровых технологий.

Ключевые слова: расследование, цифровые технологии, преступление, специальные знания, судебная экспертиза, специалист.

PODOLNY R. N., PODOLNAYA N. N.

FEATURES OF THE USE OF SPECIAL KNOWLEDGE IN DIGITAL CRIME INVESTIGATION

Abstract. Digital technologies are used in the course of committing crimes, which makes it difficult to detect the signs of criminal nature in events and facts. The subjects of criminal proceedings have problems understanding the circumstances of the commission of illegal actions. One of the means to overcome the difficulties of detecting and investigating digital crimes is to involve special knowledge in the field of digital technologies.

Keywords: investigation, digital technologies, crime, special knowledge, forensic examination, specialist.

Во всем мире сегодня наблюдается устойчивый рост внедрения и активности цифровых технологий. Сокращение численности мирового населения, не использующего Интернет, до менее чем трех млрд. человек, дает основание экспертам говорить о начале важного этапа глобальной цифровизации, когда технические приспособления с цифровыми технологиями из роскоши превратились в неотъемлемый элемент жизни человека [9]. К сожалению, современные технологии применяются и в ходе совершения преступлений, что часто осложняет деятельность правоохранительных органов по противодействию преступности. Обусловлено это тем, что применение современных цифровых технологий затрудняет восприятие в событиях и фактах признаков, указывающих на их криминальную сущность. Часто само применение таких технологий вызвано желанием замаскировать

противозаконность деяния. Но иногда задействованные технологии являются сложными настолько, что возникает вопрос о природе совершенного деяния. Как правило, этот вопрос практически всегда встает в случаях применения цифровых технологий, когда достаточно сложно определить грань между дозволенным и недопустимым поведением с точки зрения закона. Тем более, что цифровые технологии часто могут использоваться для обмана с целью завладения имуществом соответствующего лица. Они позволяют придавать внешне легальный вид намерениям конкретных лиц обогатиться преступным путем. Более того, часто с их помощью злоумышленники стремятся к тому, чтобы создать видимость благородства их поступка. Таким образом, предпринимается попытка выдать преступление за соответствующее закону действие, а иногда даже за поощряемое им.

Несомненная общественная опасность совершения преступления с помощью цифровых технологий обусловила то, что значительное число составов преступных деяний в настоящее время в качестве квалифицирующего признака предусматривают использование этих технологий. Это также повлекло выделение в Уголовном кодексе Российской Федерации [1] (далее – УК РФ) отдельной главы 28, ориентированной на защиту правоотношений в сфере компьютерной информации – «Преступления в сфере компьютерной информации». Криминализация соответствующих деяний указывает на то, что цифровые технологии, лежащие в основе компьютерной информации, являются объектом уголовно-правовой охраны. Также это позволяет сделать вывод о том, что цифровые технологии способны создавать принципиально новые правовые отношения, которые нуждаются в законодательной защите. В связи с этим можно утверждать и то, что цифровые технологии способны серьезно изменять уже существующие отношения, внося специфику в осуществление их защиты. Это, в частности, наблюдается в ст. 159.6 УК РФ, которая устанавливает уголовную ответственность за мошенничество, совершенное в сфере компьютерной информации. Отмеченную особенность цифровой информации необходимо принимать во внимание не только при квалификации названных преступлений, но и при их расследовании. При этом следует учитывать многообразие цифровых технологий в современном мире.

Существующие сегодня цифровые технологии по-разному изменяют ставшие привычными действия и отношения. Одним из востребованных видов цифровых технологий, получивших большое распространение, является технология блокчейн (blockchain) [6], которая может быть использована для записи практически всего, что имеет ценность (а не только, как это часто считается, финансовых операций с криптовалютой), а потому способна изменять сложившуюся социальную реальность и создавать как новые способы защиты от преступных посягательств, так и благоприятные для них условия.

Цифровые технологии позволяют с несколько иных точек зрения посмотреть на уже существующие и регулируемые законом отношения, привнося в них новые элементы. Они способны изменить традиционное понимание определенных социальных явлений и переосмыслить значение устоявшихся отношений для общества и государства. Это отчетливо видно на примере использования криптовалюты в конкретных правоотношениях [5]. Криптовалюта является результатом использования технологии блокчейна. Природа криптовалюты способна менять отдельные уже сложившиеся связи в сфере товарно-денежных и финансовых отношений. Она также является достаточно эффективным средством сокрытия признаков противоправности совершаемых действий. В частности, уже сами по себе операции с криптовалютой заинтересованные лица стремятся преподносить как социально-полезные, обосновывая это тем, что они способствуют ускорению экономических отношений и исключению из них излишних посредников в лице банков. Кроме того, криптовалюта позиционируется как электронные деньги, подделать которые невозможно. Это формирует у людей убеждение в безопасности вложений в криптовалюту, а потому складывается представление о том, что с ее помощью невозможно совершение преступлений, поскольку от операций с криптовалютой не может исходить какая-либо общественная опасность. Человеческая мысль не стоит на месте, и блокчейн-технологии, и сами криптовалюты также развиваются, их перспективы во многом непредсказуемы, а значит, непредсказуема и трансформация преступной деятельности, связанной с ними.

Как показывает практика правоохранительной деятельности, наиболее часто блокчейн используется при совершении мошенничества [7]. Это связано с тем, что данная технология достаточно эффективно позволяет замаскировать мотив совершения соответствующего деяния. В частности, материальные потери от криптовалюты часто представляются мошенниками как проявление нестабильности соответствующего рынка. Также преступные мотивы могут маскироваться под инвестиционные риски субъекта. В этом случае убытки представляются как результат колебаний в соответствующих отраслях экономики. Иногда убытки преподносятся как особенности конкретной криптовалюты. При этом злоумышленник стремится к тому, чтобы под сложными объяснениями сути соответствующих сделок с криптовалютой замаскировать заранее планируемые преступные действия по обращению чужих денежных средств в свою собственность.

Сложность технологий, лежащих в основе обращения криптовалюты, позволяет замаскировать под сложным объяснением корыстный мотив, ориентированный на вполне определенный преступный результат. Это позволяет злоумышленнику оправдать обращение денежных средств в свою пользу, то есть представить это как гражданско-правовую сделку. Тем самым появляется возможность обосновать отсутствие виновности лица, что будет

означать отсутствие одного из обязательных признаков преступления. Таким образом, обеспечивается не только возможность скрыть преступление, но и достаточно эффективно защититься от предъявления обвинения. Наряду с этим обеспечивается достаточно удобная позиция для планирования и организации противодействия осуществлению правосудия.

Использование цифровых технологий при совершении отдельных видов преступлений ориентировано не только на сам механизм совершения определенных действий, которые способны обеспечить достижение поставленной цели, но и на то, что сотрудники правоохранительных органов не обладают достаточным объемом знаний, необходимых для понимания соответствующих процессов и явлений. Для понимания сути действий, выполняемых с помощью цифровых технологий, недостаточно лишь юридических знаний, необходимы знания в соответствующих сферах науки и техники. Именно на это обычно и рассчитывают лица, замыслившие совершение преступления. Они полагают, что сложность и непонятность применяемой для совершения преступления технологии станет препятствием для выявления совершенного ими преступления, а в том случае, если оно и будет выявлено, то виновность будет обосновать достаточно сложно. Это ставит проблему привлечения к расследованию лиц, обладающих специальными знаниями в сфере цифровых технологий, уже на момент выявления преступления, то есть до возбуждения уголовного дела, и тесного взаимодействия следователя с этими лицами в ходе проводимого расследования. Отчасти эта проблема решается действующим уголовно-процессуальным законодательством. В частности, на стадии возбуждения уголовного дела при необходимости может быть проведена соответствующая экспертиза, в нашем случае – судебная компьютерно-техническая экспертиза, относящаяся к классу судебных инженерно-технических экспертиз [3]. Ее проведение на стадии возбуждения уголовного дела позволяет следователю еще до начала предварительного расследования определить перспективы предстоящего расследования и судебного разбирательства.

Чаще всего специальные знания в сфере цифровых технологий используются в форме проведения судебной компьютерно-технической экспертизы, несколько реже – в форме привлечения специалиста в сфере цифровых технологий, который дает пояснения фактам, событиям и обстоятельствам, устанавливаемым в ходе проводимого расследования [4]. Следственно-судебная практика показывает, что специалист по рассматриваемым уголовным делам привлекается для разъяснения участникам уголовного судопроизводства и суду вопросов, которые входят в сферу его компетенции. Однако, в соответствии со ст. 58 Уголовно-процессуального кодекса Российской Федерации [3] (далее – УПК РФ) только соответствующими разъяснениями участие специалиста в уголовном процессе не ограничивается. Для уголовного судопроизводства важны и иные компетенции специалиста,

которые достаточно четко и однозначно перечислены в названной норме уголовно-процессуального законодательства. Это, в частности, обнаружение, изъятие и закрепление предметов и документов, применение технических средств.

При расследовании преступлений рассматриваемого вида часто возникает необходимость проведения таких следственных действий, как осмотр, обыск и ряд других, результатом которых, по мысли следователя, должна стать информация, подтверждающая или опровергающая наличие значимых для дела обстоятельств. Для обеспечения успеха названных следственных действий необходимо привлечение специальных знаний в сфере цифровых технологий, поскольку без них достаточно сложно достигнуть поставленных тактических целей. Специалист в этих случаях помогает следователю в выявлении следов и иной информации, которая может способствовать восстановлению общей картины совершенного преступления или установлению его отдельных обстоятельств.

При расследовании преступлений, совершенных с применением цифровых технологий, представляется необходимым более широко использовать в деятельности следователя специальные знания. При этом недопустимо ограничиваться исключительно теми формами привлечения специалистов, которые перечислены в ст. 58 УПК РФ, а применять также и иные, которые способны оптимизировать ход расследования, обеспечив установление всех обстоятельств совершенного преступления. Практика указывает на важность тесного взаимодействия лиц, обладающих познаниями в сфере цифровых технологий, со следователем в ходе расследования преступлений названного вида. Такое взаимодействие должно обеспечивать решение тактических задач, поставленных в ходе проведения конкретных следственных действий. В связи с этим, целесообразна такая форма взаимодействия следователя со специалистом в сфере цифровых технологий, как планирование и проведение следственных действий. В результате можно будет разработать алгоритм действий, который обеспечит эффективность деятельности следователя, необходимую степень ее результативности. Кроме того, благодаря специалисту имеется возможность избежать ошибок, которые способны осложнить установление истины по конкретному уголовному делу.

Сотрудничество со специалистом в ходе расследования позволяет определять не только то, какие следственные и иные процессуальные действия могут способствовать установлению истины, но и с помощью проведения каких тактических приемов имеется возможность установления обстоятельств совершения конкретного преступления [8]. Специалист помогает определить не только наиболее эффективный алгоритм соответствующего следственного действия, но и алгоритм иных поисково-познавательных действий, проводимых следователем.

Следует особо отметить то, что одной из форм использования специальных знаний в уголовном процессе является обладание ими (пусть и в небольшом объеме) следователем. Следователь должен знать, в частности, возможности судебной компьютерно-технической экспертизы, перечень тех вопросов, на которые она способна ответить. Также следователь должен знать, какая информация может быть им получена в результате проведения соответствующих следственных действий в ходе расследования преступления, при совершении которого применялась та или иная цифровая технология. Он должен знать и то, какое противодействие установлению истины может быть оказано лицами, не заинтересованными в успешном завершении расследования. Все эти встающие перед следователем задачи могут быть эффективно решены лишь при наличии у следователя определенного минимума специальных знаний. Тогда следователь уже на начальном этапе может правильно сориентироваться в тех действиях, которые могут обеспечить успех в установлении обстоятельств расследуемого события.

Как показывает практика, нередко уже на момент поступления сообщения о совершении преступления правоохранительные органы испытывают трудности в правильном реагировании на это сообщение. Они не знают, как следует оценить соответствующее деяние по причине использования при его подготовке, совершении или сокрытии цифровых технологий, поскольку это выходит за пределы правовых знаний, которыми они обладают, и за пределы знаний о деятельности по выявлению и закреплению информации о признаках преступления. В связи с этим первоочередной задачей становится определение того, какие первоначальные действия следует предпринять при получении соответствующего сообщения о совершении преступления, в котором была применена определенная цифровая технология. Самым оптимальным способом решения указанной задачи является использование следователем своих знаний в сфере цифровых технологий, даже несмотря на то, что эти знания у него могут быть минимальны. Это позволит уже на стадии возбуждения уголовного дела заложить основы успешного предварительного расследования и последующего судебного разбирательства. Поэтому представляется целесообразным организовать соответствующее обучение следователей с тем, чтобы они обладали необходимым минимумом знаний в сфере цифровых технологий, который позволил бы правильно оценивать конкретную следственную ситуацию и планировать подходящие следственные и иные процессуальные действия.

Также следует отметить, что важным условием успешного расследования преступлений, совершенных с применением цифровых технологий, является грамотное взаимодействие следователя с лицами, обладающими соответствующими специальными познаниями. Формы и способы такого взаимодействия должны содержаться в частной

криминалистической методике расследования преступлений рассматриваемого вида. Наличие рекомендаций по использованию специальных познаний при расследовании преступлений, в которых применяются цифровые технологии, должно решить те проблемы, с которыми в настоящее время сталкивается практика правоохранительных органов. Использование названных рекомендаций способно обеспечить оптимизацию расследования преступлений рассматриваемого вида.

СПИСОК ЛИТЕРАТУРЫ

1. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 №63-ФЗ // Собрание законодательства Российской Федерации. – 1996. – №25. – Ст. 2954.

2. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 №174-ФЗ // Собрание законодательства Российской Федерации. – 2001. – №52 (часть I). – Ст. 4921.

3. Баюш А. А. Судебная компьютерно-техническая экспертиза в системе судебных экспертиз // Политехнический молодежный журнал. – 2019. – № 8 (37). – С. 10.

4. Ковалева В. А. Проблемы правового регулирования статуса специалиста и форм его деятельности в российском уголовном процессе // Современные проблемы лингвистики и методики преподавания русского языка в ВУЗе и школе. – 2022. – № 34. – С. 534–539.

5. Тихонов Э. Ю., Мухаметшина Г. Ф., Стройкина И. А. Использование криптовалют в преступной деятельности // Конкурентоспособность в глобальном мире: экономика, наука, технологии. – 2017. – № 11 (58). – С. 117–118.

6. Токолов А. В. Блокчейн-технологии в механизме преступлений в интернет-пространстве // Расследование преступлений: проблемы и пути их решения. – 2019. – № 3 (25). – С. 149–152.

7. Русскевич Е. А., Малыгин И. И. Преступления, связанные с обращением криптовалют: особенности квалификации // Право. Журнал Высшей школы экономики. – 2021. – № 3. – С. 106–125.

8. Чебуренков А. А. Проблемы оценки допустимости отдельных тактических приемов производства следственных действий // Следователь. – 2005. – № 8. – С. 24–28.

9. Kemp S. Digital 2022: July Global Statshot Report 21 July 2022 [Электронный ресурс]. – Режим доступа: https://datareportal.com/reports/?tag=Digital+2022 (дата обращения 18.09.2022).