преступлении, с одной стороны, существенно расширил возможности следователя по поиску оснований для возбуждения уголовного дела, по выявлению и фиксации доказательств. А с другой стороны, в связи с этим возникли новые проблемы процессуального и криминалистического характера, которые требуют своего скорейшего разрешения законодательным и практическим путем.

Литература

1. О внесении изменений в статьи 62 и 303 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации [Электронный ресурс]: федеральный закон от 04.03.2013 № 23-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 01.07.2021) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

М.О. Янгаева, *канд. юрид. наук*
Барнаульский юридический институт
МВД России

Тактические особенности производства обыска при расследовании преступлений, совершенных с использованием криптовалюты

При расследовании уголовных дел о преступлениях, совершенных с использованием криптовалюты, производство обыска является одним из важнейших следственных действий, результаты которого зачастую становятся ключевыми доказательствами.

Тактические особенности при расследовании рассматриваемых преступлений наблюдаются и в производстве отдельных следственных действий, в т.ч. и при производстве обыска.

При производстве обыска при расследовании преступлений, совершенных с использованием криптовалюты, основными искомыми объектами являются компьютерная техника, всевозможные носители электронной информации, денежные средства, блокноты с записями, например, логинов и паролей, финансовые документы, средства защиты информации, литература, с помощью которой была осуществлена подготовка к преступлению, другие предметы, документы, которые могут иметь значение для уголовного дела.

На подготовительном этапе производства обыска следователю необходимо:

1. Направить органу дознания поручение с целью установления:

- количества компьютерной техники, ее разновидности, которая находится в помещении, где предполагается производство обыска;
- специфики пропускного режима в организации;
- особенностей коммуникации для обмена информацией между компьютерами (наличие Wi-Fi-сети, локальной сети между компьютерами, местонахождение сервера (серверов));
- особенностей электропитания компьютерной техники и расположения мест их обесточивания;
- сведений о лицах, которые могут находиться в помещении, где предполагается производство обыска (правовой статус, образование, возраст, наличие профессиональных навыков).

2. Уточнить конкретные места и определиться со временем производства обыска, принять меры по недопущению распространения информации о подготовке к производству обыска.

3. В случаях проведения обысков в нескольких помещениях одновременно провести инструктаж участников следственной группы о порядке его производства и перечне объектов, подлежащих поиску и изъятию. Кроме того, важно организовать связь между следственными группами, находящимися на разных адресах.

4. Привлечь специалистов для производства данного следственного действия, т.к. значительная часть объектов, подлежащих поиску, – это носители компьютерной информации. Чаще всего таковыми выступают эксперты ЭКП МВД России, но могут быть привлечены специалисты и других организаций.

При производстве обыска, помимо общих требований, предъявляемых законом к его производству, следователю необходимо обратить внимание на следующие особенности:

1. Не допускать лиц, находящихся в помещении, осуществлять какие-либо действия с компьютерной техникой и электронными носителями.

2. Установить наличие сети между компьютерами, выяснить принцип ее функционирования, местонахождение серверного оборудования.

3. Изъять любые электронные носители, в первую очередь системные блоки, ноутбуки, моноблоки, оборудование для майнинга ASIC, видеокарты, жесткие диски, карты памяти различных форматов, твердотельные накопители и др. [2, с. 77].

4. Не использовать при производстве обыска устройства, которые могут издавать электромагнитное излучение, т.к. это может нанести вред информации или полностью уничтожить ее.

5. Изъятые технические устройства целесообразно упаковывать для недопущения дальнейшей работы с ними. В соответствии с требованиями ст. 164.1 УПК РФ электронные носители информации подлежат изъятию с участием специалиста [1].

Согласно ГОСТу 2.051-2013 «Единая система конструкторской документации. Электронные документы. Общие положения» электронным носителем информации является материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники.

Изучив материалы уголовных дел и мнения практических сотрудников, можно сделать вывод, что практика изъятия сотовых телефонов остается неоднозначной. Тем не менее сотовый телефон является электронным носителем информации, т.к. в нем содержится материальный носитель, используемый для записи, хранения и воспроизведения информации, поэтому целесообразно производить его изъятие также со специалистом.

Таким образом, обыск при расследовании преступлений, совершенных с использованием криптовалюты, можно отнести к числу наиболее сложных в подготовке и производстве следственных действий. Для его успешного производства необходима тщательно продуманная тактика.

Литература

1. Уголовно-процессуальный кодекс Российской Федерации: федеральный закон от 18 декабря 2001 г. № 174-ФЗ [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Янгаева М.О. Особенности изъятия электронных носителей информации при расследовании преступлений // Актуальные проблемы борьбы с преступлениями и иными правонарушениями: мат-лы восемнадцатой междунар. научно-практ. конф-ции / под ред. Ю.В. Анохина. Барнаул: БЮИ МВД России, 2020. Ч. 1. С. 76-77.