**ОСОБЕННОСТИ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОГО И НОРМАТИВНОГО СОПРОВОЖДЕНИЯ ПРОВЕДЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ «ПОЛУЧЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»**

**Шелест А.Н, студентка 1 курса магистратуры юридического института Кемгу**

**Первая особенность.** Лимитирующим фактором проведения ОРМ ПКИ, в отличие от других ОРМ, выступает техническая регламентация действия уполномоченных лиц на месте происшествия. По нашему мнению регламент должен включить в себя следующие обязательные этапы:

1) принять меры по обеспечению неизменного условия электроснабжения компьютерной техники и электронных носителей. Дело в том, что нередки ситуации, когда электронная информация утрачивается в результате аварийного отключения электропитания (например, удаление информации с буфера обмена данными, обмен данными по сети и т.п.);

2) снятие скриншотов с экрана тех программ, с которыми недавно работал заподозренный, а также изъятие системных файлов, лог-файлов, информации с журналов событий (в браузерах), то есть тех файлов, в которых фиксируются последние события на цифровых устройствах;

3) по нашему мнению, оперативный работник должен избегать любых действий, последствия которых он не может предусмотреть. Например: следует изолировать все устройства ввода данных от возможных попыток управления системой посторонних лиц;

4) решение о привлечении специалистов в области информационных технологий, а в ситуациях с шифрованием конфиденциальных данных еще и криптоаналитика или как минимум специалиста в области информационной безопасности;

5) при изъятии жесткого диска (HDD) подробно описывается место его размещения. Дело в том, что заподозренные лица размещают в системном блоке рядом с HDD либо в дверном проеме источник электромагнитных волн достаточной мощности для полного размагничивания рабочей поверхности HDD. На место осмотра и изъятия рекомендуется брать прибор по обнаружению подобных источников. Контроль над устройством ликвидации информации может быть дистанционным через специальный брелок дальностью до 1 км. и при помощи специальной кабельной линии с кнопочным механизмом с дальностью до 300 м. В Приложении 6 мы приводим перечень только некоторых наиболее часто встречаемых технических устройств, которые способны либо контактно, либо дистанционно уничтожить информацию на цифровых устройствах и носителях.

Поэтому желательно после изъятия HDD из системного блока поместить его в специальный кейс, защищенный от электромагнитных излучений. Однако во всех изученных нами материалах доследственных проверок сотрудники оперативных служб допускали одну и ту же ошибку, которая в конечном итоге приводила к отказу в возбуждении уголовного дела. Так, в материале доследственной проверки № 11-4486/2016 было установлено, что в определенном районе города Кемерово незаконно функционируют игровые автоматы. Прибывшие на место оперативные работники в первую очередь отключили от электропитания игровые автоматы и изъяли жесткие диски с игровых серверов. Исследование жестких дисков показало, что все данные на нем были уничтожены. Позже более детальный осмотр помещения позволил выявить устройство, которое размещено первым в верхнем левом углу Приложения 6;

6) также изъятию подвергается остальные обнаруженные цифровые устройства, такие как лазерные диски (CD/DVD), zip-устройства, флэш-носители и т.п. На цифровых устройствах (носителях) может содержаться: а) инсталляции программ, с помощью которых можно распознать изъятую компьютерную информацию; б) программы криптографической защиты информации; в) файлы служащие или содержащие сведения о закрытом ключе защиты цифровой информации (например, PGP, SSD, мессенджеры с технологиями чат-бот);

7) максимально снизить оперативно-разыскные риски по недопущению компрометации оперативно и криминалистически значимой информации и соответственно расконспирации работы оперативной группы. Как одна из мер - обязательное изъятие коммуникационного и иного сетевого оборудования (модем, роутер и т.п.), при его осмотре устанавливается провайдер.

После переговоров с провайдером выясняется IP-адрес абонента (заподозренного лица) и осуществляется его блокировка. Дело в том, что остается опасность входа в сеть Internet по протоколам доступа заподозренного лица. Есть вероятность, что лицо оперативной заинтересованности осуществляет преступные действия не в одиночку, а в составе преступной группы. Лица, входящие в состав преступной группы могут уничтожить или на свое усмотрение модифицировать информацию, которая имеет оперативное и криминалистическое значение, например в социальных сетях, в мессенджерах (Jabber, Telegram и др.), на удаленных серверах, облачных хранилищах и т.п. Уничтоженная и модифицированная информация будет скомпрометирована, а деятельность оперативной группы расконспирирована. Кроме того, модифицированная преступниками информация может содержать дезинформацию и пустить оперативных работников по ложному пути;

8) при изъятии компьютерной информации и ее исследовании, уполномоченное лицо должно помнить, что оперативно и криминалистически значимая информация, содержавшаяся на цифровых носителях или устройствах, может быть сокрыта от наблюдателя (методами стеганографии) и выглядеть, как что-то не привлекаемое к себе внимания, например обычный графический объект (jpeg) или ни чем непримечательный текст;

9) оперативным работникам, следователям в ситуации с недостаточным объемом поводов и оснований к проведению ОРМ ПКИ, а в особенности к возбуждению уголовного дела рекомендуем применять бесконтактные методы мониторинга за компьютерной информацией. В теории информационной безопасности известен такой метод несанкционированного доступа к конфиденциальной информации как перехват побочных электромагнитных излучений и наводок (ПЭМИН). В практике правоохранительных органов бесконтактного считывания информации через стену помещения, в котором находилось лицо оперативной заинтересованности.

**Вторая особенность.** Заключается в квалифицированной легализации результатов ОРМ ПКИ в уголовно-процессуальные доказательства. В целях фиксации некоторой части нового ОРМ, с тем, чтобы его результаты в дальнейшем могли быть применены в рамках допустимых доказательств, не рассекречивая при этом его источника, предлагаем следующие способы легализации: а) получение заключения компьютерных и иных технических экспертиз; б) получение заключения специалиста при проведении компьютерного исследования; в) в протоколе допрос специалиста); г) в протоколе осмотра цифровых устройств, телекоммуникационного оборудования, лазерных и флэш-носителей и т.п.; д) в протоколах опознания, например, скриншотов с экрана монитора, а также, при соблюдении условий безопасности для добываемой цифровой информации, аккаунтов, программных и шифровальных средств, телекоммуникационного оборудования и т.п.; е) в протоколах выемки цифровых, телекоммуникационных устройств, цифровых носителей и т.п.

**Третья особенность.** Заключается в целесообразности выделения проведения компьютерного исследования информации добытой в рамках ОРМ ПКИ. Целесообразность состоит в следующем:

1) компьютерное исследование допустимо проводить в рамках доследственной проверки;

2) результаты компьютерного исследования могут послужить достаточными основаниями к возбуждению уголовного дела;

3) оптимизация некоторых способов легализации результатов ОРМ ПКИ;

4) может служить основанием к продлению сроков рассмотрения сообщения о преступлении до 30-ти суток (в рамках ч. 3 ст. 144 УПК);

5) достигается сохранность объектов и иных документов при проведении компьютерной экспертизы.

Предложенные нами способы легализации результатов нового ОРМ будут способствовать значительном увеличению количества раскрываемых преступлений по изучаемой категории уголовных дел и проходят пробационное внедрение в подразделениях полиции Кемеровского районы, где по нашим данным осуществляется значительное количество «закладок» на территории сельских поселений, турбаз и т.п.

Мы должны признать, что основными угрозами государственной и общественной безопасности являются: деятельность преступных организаций и группировок, в том числе транснациональных, связанная с незаконным оборотом наркотических средств и психотропных веществ, оружия, боеприпасов, взрывчатых веществ, организацией незаконной миграции и торговлей людьми[[1]](#footnote-1).

Список литературы:

1. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации».

1. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации». [↑](#footnote-ref-1)