**Теоретические и прикладные аспекты информационной безопасности** : материалы Междунар. науч.-практ. конф. (Минск, 31 марта 2016 г.) / учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь» ; редкол.: А.В. Яскевич (отв. ред.) [и др.]. – Минск : Академия МВД, 2016. – 419, [1] с. – С. 138-141 (тезисы)

УДК 343.98

*Хлус А.М.*, *Бичун В.М.*

# ТИПИЧНЫЕ СЛЕДСТВЕННЫЕ СИТУАЦИИ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационные системы стали неотъемлемой частью объектов материальной среды практически во всех сферах деятельности человека. Это связано с повышением роли компьютерной техники в современной жизни человечества, развитием программно-технических средств и массовым овладением компьютерами.

Вычислительная техника с огромными производительными возможностями обусловила компьютеризацию экономической, управленческой, научной и иных сфер деятельности. Использование компьютерной техники в космических исследованиях, в оборонной промышленности, в атомной энергетике и других областях жизни общества поставило перед человечеством проблему обеспечения ее надежности и защиты.

Преступность в сфере информационной безопасности все больше дает о себе знать во всем мире и наша республика не является исключением. Специфичность преступлений в сфере информационной безопасности, многообразие способов преступных действий, их высокая латентность создали в этой сфере для правоохранительных органов достаточно сложное поле деятельности на пути к защите прав и интересов общества и государства.

В следственной ситуации как объективно существующей системе условий и обстоятельств, которые складываются на конкретный момент

расследования преступлений, обычно выделяют такие наиболее важные ее составляющие элементы, как сведения об общественно опасном деянии и лице, его совершившем. Для преступлений против информационной безопасности типичные ситуации первоначального этапа расследования включают также сведения о способе их выявления.

В учебной литературе по криминалистике упоминаются три типичных следственных ситуации, характерных для первоначального этапа расследования преступлений в сфере информационной безопасности:

1. Собственник компьютерной системы обратился в правоохранительные органы с заявлением о несанкционированном доступе в компьютерную систему либо завладении конфиденциальной информацией, содержащейся в ней. Виновное лицо неизвестно.

2. Собственник компьютерной системы обратился в правоохранительные органы с заявлением о несанкционированном доступе в компьютерную систему либо завладении конфиденциальной информацией, содержащейся в ней. Виновное лицо известно.

3. Данные о нарушении целостности либо конфиденциальности информации в компьютерной системе и виновном лице стали общеизвестными или непосредственно обнаружены правоохранительными органами (например, в ходе оперативно-розыскных мероприятий или расследования другого уголовного дела).

Первая следственная ситуация характеризуется бесконфликтностью. В этом случае отсутствует сторона, препятствующая расследованию уголовного дела. Вместе с тем эта ситуации является неблагоприятной, так как имеющейся информации недостаточно для установления лиц, причастных к преступлению, их виновности и других обстоятельств, подлежащих доказыванию по уголовному делу.

Вторая и третья следственные ситуации более благоприятны для расследования, так как установлено лицо, подозреваемое в совершении

преступления. Это позволяет провести следственных действий с его участием. Также проводятся оперативно-розыскные и иных мероприятия, направленные на проверку причастности конкретного лица к деяниям, посягающим на информационную безопасность.

В ходе расследования следственные ситуации могут стать конфликтными, если подозреваемое лицо отказалось от дачи показаний, попыталось направить следствие по ложному пути или приняло иные меры, направленные на сокрытие своей причастности к преступлению.

В ходе расследования преступления в любой из перечисленных следственных ситуаций необходимо соблюдать следующие важные требования.

Во-первых, расследование целесообразно проводить лицу, которое на высоком уровне владеет знаниями о компьютерной технике. В противном случае необходимо обеспечить участие специалиста в проведении любого следственного действия, связанного с исследованием компьютеров. Следует помнить, что неквалифицированные действия в компьютерной системе могут привести к безвозвратной утрате ценной доказательственной информации. Как показывает практика, наиболее полезно участие специалиста в следственном осмотре, обыске и выемке, следственном эксперименте, а также при подготовке к проведению допроса. При подготовке к проведению допроса особое значение имеет уяснение следователем особенностей работы тех или иных средств компьютерной техники. Важным является и уточнение с помощью специалиста специальной терминологии, применяемой в данной сфере.

Во-вторых, необходимо, обеспечить оперативное сопровождение процесса предварительной проверки первичной информации и расследования вплоть до момента направления дела прокурору, а при необходимости – и до вынесения приговора. В этой связи по данной категории дел очень велика роль взаимодействия между следователем и сотрудниками оперативных подразделений. Проводя оперативно-розыскные мероприятия, оперативный работник должен вести активный поиск источников получения доказательств

совершенного преступления, выявлять ранее неизвестных свидетелей, устанавливать лиц, которые могут быть причастны к преступлению, проверять их алиби, связи, принимать меры к обнаружению мест хранения средств совершения преступления, имущества, денег и других ценностей, нажитых преступным путем.

При получении материалов оперативно-розыскной деятельности, содержащих криминалистически значимую информацию, следователь должен их легализовать посредством проведения соответствующих следственных действий и процессуально оформить в качестве доказательств. При этом между следователем и оперативными работниками должен быть налажен своевременный обмен информацией обо всех без исключения действиях (мерах), которые они намерены провести, и проводят, и о полученных материалах, иначе указанные субъекты могут непреднамеренно помешать друг другу и тем самым осложнить расследование.

Безусловно, в ходе расследования преступлений в сфере информационной безопасности необходимо использовать весь комплекс следственных действий предусмотренных уголовно-процессуальным законом. При наличии достоверных данных о преступнике программа расследования включает следующие действия: задержание подозреваемого, следственные осмотры, допросы подозреваемого, потерпевших, свидетелей; обыски и выемки с целью обнаружения средств совершения преступления, предметов и документов, которые могут иметь значение для дела; проверку показаний на месте, следственный эксперимент, наложение ареста на почтово-телеграфные и иные отправления, их осмотр и выемка, различные экспертизы (как криминалистические, так и компьютерно-технические, компьютерно-технологические и т.д.). Также необходимо проведение комплекса оперативно-розыскных мероприятий, направленных на установление связей подозреваемого, мест сокрытия средств совершения преступления, обстоятельств совершения преступления. При отсутствии данных о

преступнике осуществляются следственные осмотры, среди которых большое значение имеют осмотр места происшествия; допросы потерпевших и свидетелей; следственный эксперимент; экспертизы; прослушивание и запись переговоров. Осуществляется также комплекс мероприятий, направленных на установление и розыск подозреваемого в совершении преступления, его задержание. В зависимости от ситуации также проводятся другие следственные действия и оперативно-розыскные мероприятия.

Рассмотренные выше ситуации характерны для случаев, когда преступник находится и совершает преступление в пределах государства. Но если учесть, что преступления против информационной безопасности носят трансграничный характер, то следует выделить и рассмотреть еще одну следственную ситуацию. Для нее характерно наличие сведений о том, что преступному воздействию подверглась компьютерная система, а преступник либо преступная организация находятся за пределами границ Республики Беларусь. Преступные деяния могут быть выявлены как собственником компьютерных систем, так и оперативными подразделениями. Перспектива расследования таких преступлений зависит от многих факторов. Во-первых, успешно противодействовать таким преступлениям могут подразделения, специально созданные для борьбы с так называемой «киберпреступностью». Во-вторых, деятельность национальных органов, осуществляющих оперативно-розыскную деятельность, будет не эффективной, если отсутствует взаимодействие с аналогичными зарубежными спецслужбами.

Следует также иметь в виду, что информационная сфера является полем современной информационной войны, в рамках которой осуществляются деяния различной целевой направленности, что, в свою очередь, определяет направления, средства и методы противодействия.