ПРОТИВОДЕЙСТВИЕ РАССЛЕДОВАНИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ НА СТАДИИ ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА

Д.А. Першин, АлтГУ, юридический факультет, 5 к.
Научный руководитель – ***В.В. Поляков,*** к.ю.н., доцент.

Преодоление противодействия на стадии возбуждения уголовного дела связано с тем, что преступники стремятся предпринять действия, препятствующие выявлению и расследованию преступления.

Возбуждение уголовного дела предполагает наличие определенной информации, из которой можно сделать вывод о том, что преступление действительно имело место. Данная информация может быть получена уполномоченными на это оперативными сотрудниками, которые передают ее органу следствия. Далее, следователь оценивает эту информацию и принимает решение о возбуждении уголовного дела. В случае, когда поводом или основанием для возбуждения уголовного дела явилось другое обстоятельство, например, заявление потерпевшего, следователь не может занимать пассивную позицию, он должен четко обозначить какую именно информацию ждет от оперативников, проанализировать ее на предмет достоверности, и подумать над тем, какие действия предпринять, чтобы расследование было успешным. Следователь может дать письменное поручение о производстве оперативно-розыскных мероприятий. Как показывает практика расследования уголовных дел по компьютерным преступлениям, такие обращения редко облекаются в письменную форму, а ограничиваются устной просьбой о необходимости получения дополнительной информации. Подобная практика увеличивает оперативность, и способствует соблюдению процессуальных сроков.

Опытные преступники, информированные о протекании расследования, стараются найти в нем уязвимые места для применения мер противодействия [1]. Обычно, с их стороны предпринимаются следующие действия:

1. Дистанционное уничтожение электронных документов или иной информации, хранящейся на компьютере или носителе информации;

2. Создания документов-двойников с целью формирования иллюзии о том, что документ, в котором правоохранительные органы видят информацию о преступлении, на самом деле свидетельствует об обратном;
3. Внесение изменений в учетные и иные данные в программной среде компьютера. Так, например, уничтожается информация, свидетельствующая о неправомерном доступе, или подкидывается информация, которая направляет правоохранительные органы на ложный след, указывающий, что преступление совершено иным лицом;
4. Развертывание в СМИ дискуссии о допустимости действий, схожих с теми, которые составляют конкретное преступление, выявлением или расследованием которого в данный момент занимаются правоохранительные органы. Эти действия рассчитаны на то, чтобы сформировать общественное мнение о несправедливости возможного уголовного преследования, повлиять на взгляды сотрудников правоохранительных органов;
5. Воздействие на конкретных сотрудников правоохранительных органов (нахождение коррупционных и приятельских связей) [2].

С целью преодоления противодействия со стороны преступника и лиц, сочувствующих ему, необходимо соблюдение полной конспирации о планируемых и совершаемых действиях, направленных на сбор информации, которая необходима для решения вопроса о возбуждении уголовного дела. Н.А. Подольный справедливо отмечает, что необходимость конспирации в случае проведения оперативно-розыскных мероприятий с целью выявления компьютерных преступлений является важнейшим условием получения достоверной информации [3]. От потерпевших необходимо потребовать не разглашать сведения, которые могли стать им известны от правоохранительных органов.

Во время принятия решения о возбуждении уголовного дела оперативные сотрудники должны выяснить возможность последующего получения доказательств в результате следственных действий, так как нередки случаи, когда до возбуждения уголовного дела лица дают объяснения, прямо указывающие на виновность

конкретного субъекта, а после возбуждения уголовного дела дают прямо противоположные показания.

Для решения вопросов о преодолении противодействия в стадии возбуждении уголовного дела о преступлениях в сфере компьютерной информации целесообразно привлечение специалистов [4]. С их помощью сформировывается представление не только об общей картине совершенного преступления, но и опасностях, которые могут подстерегать следствие при сборе доказательств [5].

Проблема противодействия расследованию преступлений в сфере компьютерной информации, особенно на стадии возбуждения уголовного дела, является малоизученной и требует дальнейшего исследования.

Список литературы

1. Поляков В.В. Следственные ситуации по делам о неправомерном удаленном доступе к компьютерной информации // Доклады Томского государственного университета. 2010. N1(21). С. 46 - 50.
2. Преодоление противодействия расследованию преступлений в сфере компьютерной информации: монография / под ред. Н.А. Подольного. М.: Юрлитинформ, 2013. – 216 с.
3. Подольный Н.А. Ширманов А.Г. Некоторые особенности выявления, раскрытия и расследования компьютерных преступлений // Российский следователь 2004. №1. С. 11.
4. Поляков В.В. Криминалистическая структура мер предупреждения компьютерных преступлений // Библиотека криминалиста: научный журнал. 2013. №5 (10). С. 287 - 291.
5. Поляков В.В. Особенности подготовки специалистов для расследования преступлений, связанных с неправомерным удаленным доступом к компьютерной информации // Известия Алтайского государственного университета. 2010. N 2/1. С. 96 - 97.