***Ю.А. Егоров**, канд. юрид. наук, доцент,*
БГЭУ (г. Минск)

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ

Преступления в сфере информационной безопасности носят латентный характер, не оставляют, как правило, видимых следов и сложны с точки зрения их раскрытия и собирания доказательственной информации. Данные обстоятельства отражаются на специфике раскрытия и расследования преступлений в данной сфере.

Одной из основных проблем и особенностей при раскрытии и расследовании преступлений данной группы является установление самого факта совершения преступного деяния в сфере информационной безопасности и неправомерных действий лиц, посягающих на охраняемую законом информацию.

Анализ правовых норм, а также материалов практики расследования преступлений в данной сфере позволяет сделать один весьма значимый вывод. Согласно действующего уголовного законодательства данные преступления в своей основной массе не представляют большой общественной опасности, следовательно, согласно Уголовно-процессуального кодекса Республики Беларусь, мера пресечения в виде заключения под стражу не применяется за исключением случаев, предусмотренных законом. Следовательно, данное обстоятельство может оказать влияние на ход расследования по уголовному делу в виде противодействия правоохранительным органам, к примеру, путем уничтожения доказательственной базы, уговоров, запугивания свидетелей и др. Поэтому на первый план при раскрытии и расследовании преступлений данной группы выходит оперативная работа правоохранительных органов по выявлению признаков преступления, лиц их совершивших и возможных свидетелей, а также подготовке мероприятий по сбору доказательств. И на момент возбуждения уголовного дела необходимо, по возможности, провести комплекс перечисленных выше мероприятий с целью возможной нейтрализации противодействия процессу расследования и обеспечения получения доказательств.

При расследовании преступлений в сфере информационной безопасности, обычно выделяется три типичных следственных ситуации, складывающихся на первоначальном этапе:

1. Собственник компьютерной системы собственными силами выявил нарушение целостности (конфиденциальности информации в системе), обнаружил виновное лицо и заявил об этом в правоохранительные органы.

2. Собственник компьютерной системы собственными силами выявил нарушение целостности (конфиденциальности информации в системе), не смог обнаружить виновное лицо и заявил об этом в правоохранительные органы.

3. Данные о нарушении целостности (конфиденциальности информации в компьютерной системе) и виновном лице стали общеизвестными или непосредственно обнаружены органом дознания (например, в ходе проведения оперативно-розыскных мероприятий).

В ходе расследования преступления в любой из перечисленных следственных ситуаций необходимо иметь в виду несколько важных моментов. Первое – это обязательное участие специалиста в проведении любого следственного действия связанного с манипуляциями с ЭВМ, т. к. малейшие неквалифицированные действия с компьютерной системой могут закончиться безвозвратной утратой ценной доказательственной информации. При этом, как показывает практика, наиболее полезно участие специалиста в следственном осмотре, обыске и выемке. Второе – необходимо оперативное сопровождения дела с момента получения первичной информации и до момента направления дела прокурору. Именно по данной категории дел очень велика роль взаимодействия между следователем и сотрудниками оперативного аппарата. Проводя оперативно-розыскные мероприятия, оперативный работник должен вести активный поиск источников получения доказательств совершенного преступления, выявлять ранее неизвестных свидетелей, проводить проверку лиц, которые могут быть причастными к преступлению, установление их алиби, связей, принимать меры к обнаружению мест хранения орудий и средств преступления, имущества, денег и других ценностей, нажитых преступным путем [1, с. 142–143].

Следователь при получении такого рода информации должен путем проведения соответствующих следственных действий процессуально оформить ее в виде доказательств. При этом между следователем и оперативным работником должен быть налажен своевременный обмен информацией о всех без исключения действиях (мерах), которые они намерены провести и проводят, и о полученных результатах. Иначе следователь и оперативный работник могут непреднамеренно помешать друг другу и тем самым осложнить расследование [2, с. 8].

Специфика расследования преступлений в сфере информационной безопасности обуславливает необходимость применения специальных знаний в форме проведения экспертного исследования. Причем, в ряде случаев, по нашему мнению, необходимо проведение экспертизы до возбуждения уголовного дела для решения вопроса о его возбуждении в ходе проведения доследственной проверки по собранным материалам. Следует отметить, что закон позволяет нам проводить экспертизу до возбуждения уголовного дела и, следовательно, правоохранительные органы должны активно использовать данную возможность для сбора доказательств и ввода их в сферу уголовного процесса. Экспертное исследование также может быть назначено непосредственно после возбуждения уголовного дела как одно из неотложных следственных действий, проводимых на первоначальном этапе расследования. Формой использования специальных знаний по данной категории дел, как правило, является проведение компьютерно-технической экспертизы.

Обобщая сказанное, представляется возможным сделать следующие выводы:

1. Анализ специфики расследования преступлений в сфере информационной безопасности позволяет говорить о необходимости сбора качественного материала доследственной проверки, на основании которого возможно возбуждение уголовного дела, его быстрое расследование и направление в суд. При этом на первый план выходит работа оперативных аппаратов по сбору такого материала и его последующей реализации.

2. В ходе возбуждения уголовного дела необходимо заранее быть готовыми к открытому и скрытому противодействию фигурантов по уголовному делу, а также со стороны их родственников и знакомых, поэтому до возбуждения уголовного дела необходимо проведение комплекса подготовительных мероприятий, направленных на получение доказательств и обеспечение их использования в сфере уголовного судопроизводства, а также нейтрализацию противодействия процессу расследования.

3. Необходимо обязательное участие специалиста в проведении любого следственного действия, связанного с манипуляциями с ЭВМ, а также проведение консультационной работы специалистом при осуществлении и подготовке иных следственных действий. Данное правило является обязательным и направлено на обеспечение сохранности доказательственной информации и более качественное проведение следственных действий.

4. Для объективности и полноты расследования по делам данной категории назначать и проводить компьютерно-техническую экспертизу до возбуждения уголовного дела (ст. 173 ч. 2 и ст. 226 ч. 2 УПК Республики Беларусь) или непосредственно после возбуждения уголовного дела как одно из неотложных следственных действий, проводимых на первоначальном этапе расследования.

Список использованных источников

1. Вехов, В.Б. Компьютерные преступления: Способы совершения и раскрытия / В.Б. Вехов; под ред. акад. Е.Л. Смагоринского. – М.: Право и Закон, 2006. – С.142–143.

2. Сорокотягин, И.Н. Понятие и виды взаимодействия следователя и сведущих лиц / И.Н. Сорокотягин. – Свердловск: Университетское, 1989. – 8 с.

***В.Н. Завгородняя**, канд. юрид. наук, доцент,*
ГВУЗ «Украинская академия банковского дела Национального банка Украины»
(г. Сумы, Украина)

ПОНЯТИЕ ЕВРОПЕЙСКОГО АДМИНИСТРАТИВНОГО ПРОСТРАНСТВА

В современном мире глобализация касается всех сфер общественной жизни, в том числе и функционирования публичной администрации, деятельность которой ранее традиционно считалась исключительной внутренней прерогативой государства. Указанные тенденции дали основание многим исследователям ставить вопрос о формировании глобального административного пространства и даже глобального административного права [1, 2, 3].