Хлус, А. М. Особенности методического обеспечения борьбы с преступлениями в сфере информационных технологий / А. М. Хлус // Проблемы получения и использования доказательственной и криминалистически значимой информации : материалы Междунар. науч.-практ. конф., 26–27 сентября 2019 г., Мисхор (Большая Ялта) / отв. ред. М. А. Михайлов, Т. В. Омельченко; Крымский федеральный университет имени В. И. Вернадского. – Симферополь : ИТ «АРИАЛ», 2019. – С. 109–112.

Хлус Александр Михайлович,
Белорусский государственный университет,
кандидат юридических наук, доцент,
(Минск, Республика Беларусь)

Особенности методического обеспечения борьбы с преступлениями в сфере информационных технологий

УДК 343.98

Аннотация

Технический прогресс способствовал появлению единого информационного пространства. Его формирование связано с расширением преступного интереса в информационной сфере. Это повлекло за собой появление преступлений в сфере информационных технологий.

Результативность борьбы с преступлениями в сфере информационных технологий предполагает наличие разработанных методик раскрытия и расследования преступлений данной группы.

Существующее методическое обеспечение раскрытия и расследования преступлений в сфере информационных технологий, основанное на их криминалистической характеристике, не удовлетворят потребностям времени. Предлагается формировать частных методик расследования преступлений данной группы на основе первоначального выявления и дальнейшего описания материальных элементов, составляющих структуру данных преступных деяний.

Ключевые слова: *информационное пространство; криминалистика; методика расследования преступлений; криминалистическая характеристика преступлений; материальная структура преступлений.*

Features of methodological support of the fight against crimes in the field of information technology

Khlus A.

Annotation

Technological progress has contributed to the emergence of a single information space. Its formation is associated with the expansion of criminal interest in the information sphere. This led to the emergence of crimes in the field of information technology.

The effectiveness of the fight against crimes in the field of information technology suggests the existence of developed methods for the disclosure and investigation of crimes of this group.

The existing methodological support for the disclosure and investigation of crimes in the field of information technology, based on their forensic characteristics, will not satisfy the needs of the time. It is proposed to formulate private methods for investigating the crimes of this group on the basis of the initial identification and further description of the material elements that make up the structure of these criminal acts.

Keywords: *information space; forensic science; crime investigation methodology; forensic characteristics of crimes; material structure of crimes.*

Развитие информационных технологий способствовало возникновению новых социальных явлений, как позитивных, так негативных. В аспекте нашего исследования обратим внимание на такие негативные явления как преступления в сфере информационных технологий.

Борьба с преступлениями в сфере информационных технологий не являются только государственной проблемой, она имеет международный характер. Мировое сообщество озабочено данной проблемой и принимает различные меры, направленные на ограничение развития этих преступлений. Достижение этой цели зависит от многих условий, в том числе и от политической воли руководства отдельных государств.

В Республике Беларусь проводится планомерная и последовательная политика борьбы с преступлениями в сфере информационных технологий. Вместе с тем кроме политических решений, необходимы действенные меры, обеспечивающие эффективную борьбу с этими преступлениями. Разработка и внедрение в практическую деятельность этих мер имеет также и экономическое значение.

Экономический интерес является одним из направлений преступной деятельности в информационном пространстве. Например, пресс-служба МВД Беларуси сообщила о волне посягательств на белорусские предприятия [1].

Снижение уровня совершаемых преступлений в информационном пространстве будет способствовать появлению позитивных сдвигов в перспективе экономического, инвестиционного и инновационного развития Беларуси.

Одной из составляющих эффективной борьбы с преступлениями в сфере информационных технологий является наличие соответствующей законодательной базы, способствующей должному реагированию на все виды этих преступлений.

В действующем законодательстве Республики Беларусь отсутствует представление о понятии «преступление в сфере информационных технологий». Наряду с данным понятием в научной среде и практической деятельности используется термин «киберпреступность», который не имеет единообразного понимания. Понятия «преступления в сфере информационных технологий» и «киберпреступность» учеными и практиками используются как синонимы. По мнению Т.Л. Тропининой «киберпреступность – совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей или компьютерных данных» [2, с. 20].

Данная формулировка на сегодняшний день представляется не отражающей действительность, так как в ней говорится о совершении противоправного деяния только с «помощью или посредством компьютерных систем или сетей». В настоящее время киберпреступления могут совершаться с использованием иных технических средств, например, мобильных телефонов. По нашему мнению в определении понятия «киберпреступность» должно присутствовать указание на совершение преступлений в сфере IT-технологий. А совершаемое преступное деяние направлено не только «против компьютерных систем, компьютерных сетей или компьютерных данных». Оно может быть связано с посягательством на отдельную личность (клевета или оскорбление в сети Интернет), неопределенное количество лиц (распространение экстремистских материалов) и т.д.

В связи с наличием множества незаконных деяний, совершаемых в информационном пространстве, представляет интерес высказанное Ивановой Л.В. мнение о необходимости включения во все статьи УК Российской Федерации квалифицирующего признака совершения деяния «с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет», за исключением тех преступлений, которые

даже теоретически не могут быть совершены посредством IT-технологий [3, с. 32]. Данная рекомендации заслуживает внимания со стороны законодателя в аспекте совершенствования действующего уголовного законодательства многих государств, в том числе и Республики Беларусь.

В Уголовном кодексе Республики Беларусь (далее УК) предусмотрена ответственность за ряд деяний, которые следует признать преступлениями в сфере информационных преступлений (киберпреступлениями). УК Республики Беларусь содержит ряд статей, предусматривающих ответственность за преступления против собственности (ст. 212 УК) и информационной безопасности (ст. 349-355 УК), совершенные с использованием компьютерных технологий.

Развитие современной техники определяет необходимость внесения изменений в указанные выше статьи уголовного кодекса, которые в теории криминалистики относят к группе «компьютерных преступлений» [4]. Компьютерные преступления являются разновидностью преступлений в сфере информационных технологий, которые значительно шире по охвату совершаемых в информационном пространстве преступных деяний.

Эффективность деятельности по расследованию преступлений в сфере информационных технологий, на наш взгляд, во многом зависит от наличия современной, научно разработанной частной криминалистической методики.

Существующие методики расследования преступлений в сфере IT-технологий не совершенны. Связано это с рядом специфических признаков этих преступлений. Во-первых, во многих случаях они имеют международный характер (выходят за пределы одного государства). Во-вторых, существуют проблемы в определении места совершения преступления. В-третьих, наличествуют «слабые связи между уровнями и звеньями в системе доказательств» [5]. В-четвертых, не воспринимаемая визуально следовая картина преступления, совершенного в информационном пространстве. Все это создает проблему для формирования информационной основы для

разработки частной криминалистической методики раскрытия и расследования преступлений в сфере IT-технологий.

Для построения частных криминалистических методик в качестве информационной модели преступления чаще используется его криминалистическая характеристика. Учитывая, мобильность преступлений в сфере IT-технологий, их способность к активной модификации, что влечет за собой появление не только новых способов, но и по сути новых преступлений, невозможно осуществить наиболее объективное описание (дать криминалистическую характеристику) конкретного вида информационных преступлений. Более того, в настоящее время, криминалистическую характеристику преступлений ученые воспринимают как абстрактное понятие [6, с. 223].

Не высокий уровень значимости криминалистической характеристики преступления для практической деятельности привел к пониманию необходимости осуществления познания преступлений на иной основе. Такой основой служит материальная структура преступления.

Построение данной информационной модели отдельного вида и группы преступлений, а затем ее использование в процессе раскрытия и расследования конкретного криминального события, предлагается на основе знаний о его уголовно-правовом составе [7, с. 612].

Знание материальной структуры преступлений представляет интерес не только для развития теории криминалистики, но также значимо для практической деятельности по расследованию. Она определят целенаправленность и последовательность в работе следователей.

Структура каждого вида преступлений различна. Отличаются характеристики и свойства элементов совершения уголовных преступлений. В преступлениях одного вида может различаться количественный состав элементов.

Как представляется, в содержании материальной структуры преступлений в сфере информационных технологий (например, преступлений против

информационной безопасности) можно выделить следующие общие элементы: субъект и объект преступного посягательства, средство совершения преступления и предмет преступления.

В качестве субъекта совершения любого преступления в сфере информационных технологий может рассматриваться только человек. Отличительная особенность субъекта, как элемента структуры данных преступлений, в том, что он может рассматриваться преимущественно как следообразующий элемент. В качестве следовоспринимающего элемента его можно рассматривать по отношению только к средству совершения преступления.

Иные материальные элементы в структуре преступлений в сфере информационных технологий рассмотрим на примере ст. 350 УК. Часть 1 указанной статьи предусматривает уголовную ответственность за «изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред при отсутствии признаков преступления против собственности» (модификация компьютерной информации).

В качестве объектов преступного посягательства (преступления) с точки зрения криминалистической науки, в отличие от уголовного права, следует рассматривать не общественные отношения, а те материальные элементы в структуре преступления, на которые преступник оказывает воздействие. Такими объектами норма уголовного права называет компьютерную систему, сеть или машинные носители информации. Именно данные материальные элементы содержат следовую информацию о действиях преступника, представляющую интерес для криминалистики и, соответственно, для расследования преступления. Но для ч. 1 ст. 350 УК названные элементы можно рассматривать в качестве объекта посягательства только в случае, когда действия виновного связаны с изменением информации либо внесением заведомо ложной информации в компьютерную систему и т.д. Дело в том, что ч. 1 ст. 350 УК предусматривает уголовную ответственность для лиц, которые

имеют разрешенный, т.е. санкционированный доступ к работе в компьютерной системе, сети или на машинных носителях информации. В «чистом» виде компьютерную систему или сеть можно рассматривать объектами посягательства, когда имеет место несанкционированный доступ к ним, что влечет за собой уголовную ответственность по части 2 ст. 350 УК за действия связанные с модификацией компьютерной информации. Ответственность за «несанкционированный доступ» предусмотрена также ч. 1 ст. 349 УК, когда такой доступ повлек по неосторожности изменение, уничтожение, блокирование компьютерной информации или вывод из строя компьютерного оборудования.

«Изменение информации» является целью преступных действий, что определяет ее как предмет преступления.

В ч. 1 ст. 350 УК содержится указание на возможность совершения действий, связанных с внесением «заведомо ложной информации» в компьютерную систему, сеть или на машинный носитель информации. Данный элемент в преступной структуре представляет собой средство совершения преступления. В качестве средств, при совершении иных преступлений в сфере информационных технологий, может выступать компьютерная техника (ст. 349 УК «Несанкционированный доступ к компьютерной информации»), программные (аппаратные) средства, обеспечивающие доступ к защищенной компьютерной системе или сети (ст. 353 УК «Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети»), вредоносные программы (ст. 354 УК «Разработка, использование либо распространение вредоносных программ»).

Выделение элементов материальной структуры преступлений против информационной безопасности, а затем их анализ обеспечивают наиболее полное и объективное познание конкретного преступления.

При развитии следственной ситуации, когда субъект преступления не известен, его познание и других элементов структуры конкретного преступления против информационной безопасности начинается с

исследования объекта посягательства. Исследование компьютерной системы, сети или машинных носителей информации посредством изучения следов преступления позволяет выявить особенности обстановки преступного посягательства и установить конкретный способ совершения преступления.

Система следов, отразившихся на объекте преступного посягательства от иных структурных элементов преступления, образует так называемую следовую картину. Ее анализ при расследовании преступлений данного вида позволяет сделать вывод, что в качестве следов могут выступать: 1) изменения исходной информации на магнитных и оптических носителях; 2) следы уничтожения или блокирования информации; 3) следы опосредованного доступа к ней с помощью глобальных или локальных компьютерных сетей [8, с. 247]. Нетрадиционный характер этих следов привел к предложению ввести понятие «виртуальный след» [9, с. 59].

На основе изучения следовой картины конкретного преступления выявляется связь между способом совершения преступления, свойствами субъекта посягательства и обстановкой, в которой совершено преступное деяние данным способом.

Сведения о способе и обстановке совершения преступления образуют информационную основу криминалистической характеристики преступлений в сфере информационных технологий. Их использование при исследовании объекта преступного посягательства позволяет следователю выдвинуть наиболее вероятную версию о субъекте совершения преступного деяния. Так, например, для крэкеров характерно использование способов, направленных на получение несанкционированного доступа к компьютерной информации [8, с. 238]. Их основной задачей является взлом компьютерной системы с целью получения несанкционированного доступа к чужой информации.

На основании изложенного предлагаются следующие выводы:

Во-первых, результативность деятельности правоохранительных органов в борьбе с преступлениями в сфере информационных технологий зависит от

наличия разработанных на научной основе методик раскрытия и расследования преступлений данной группы.

В-вторых, методическое обеспечение раскрытия и расследования преступлений в сфере информационных технологий, основанное на их криминалистической характеристике, не соответствует современному времени.

В-третьих, формирование частных методик раскрытия и расследования преступлений в сфере информационных технологий должно основываться на первоначальном выявлении и дальнейшей характеристике (описании) материальных элементов в структуре данных преступных деяний.

Список использованных источников

1. МВД Беларуси заявляет о волне кибератак на белорусские предприятия. [Электронный ресурс]. – Режим доступа: https://interfax.com.ua/news/general/603530.html. (дата обращения: 02.08.2019).

2. Тропинина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы. Дис. … канд. юрид. наук. – Владивосток, 2005. – 234 с.

3. Иванова Л.В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. – № 1. – С. 28–32.

4. См. напр. Козлов В.Е. Компьютерные преступления: криминалистическая характеристика и осмотр места происшествия: Моногр. – Мн.: Акад. МВД Республики Беларусь, 2001. – 120 с.

5. Кравцова М.А. Понятие киберпреступности и ее признаки. [Электронный ресурс]. – file:///C:/Users/Admin/Downloads/Chkup_2015_2_78.pdf. (дата обращения: 06.08.2019).

Кравцова М.А. Понятие киберпреступности и ее признаки. [Электронный ресурс]. – file:///C:/Users/Admin/Downloads/Chkup_2015_2_78.pdf. (дата обращения: 06.08.2019).

6. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики / М.: Издательство НОРМА (Издательская группа НОРМА-ИНФРА · М), 2001. – 240 с.

7. Хлус А.М. Уголовно-правовые основы построения информационной модели преступления / Актуальні проблеми криминальноі відповідальності: матеріали междунар. науч.-практ. конф., 10-11 жовт. 2013 р. / редкол. : В. Я. Тацій (голов. ред.), В. І. Борисов (заст. голов. ред.) та ін. – Х. : Право, 2013. – С. 610–614.

8. Криминалистика : учебник : в 3 ч. Ч. 3. Криминалистическая методика / под ред. Г.Н. Мухина ; М-во внутрен. дел Респ. Беларусь, учреждение образования «Акад. М-ва внутрен. дел Респ. Беларусь». – 2-е изд., испр. – Минск : Акад. МВД, 2010. – 295 с.

9. Ищенко Е.П. Об актуальных проблемах технико-криминалистического обеспечения расследования преступлений / Актуальные проблемы современной криминалистики и судебной экспертизы : материалы Междунар. науч.-практ. конф., посвящ. 35-летию со дня образования кафедры криминалистики Акад. МВД Республики Беларусь (Минск, 3 июня 2011 г.) / М-во внутр. дел Респ. Беларусь, учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь» ; редкол.: Н.И. Порубов [и др.].– Минск : Акад. МВД, 2011. – С. 58–59.