УДК 343.98

М. Н. АНДРЕЙЧУК
Брест, БрГУ имени А. С. Пушкина
Научный руководитель – И. А. Заранка, магистр юрид. наук,
старший преподаватель

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Научно-технический прогресс повлек за собой серьезные социальные изменения, в результате которых возник новый вид общественных отношений и особых ресурсов – информационных. Развитие и тенденции преступности затрагиваются как процессом глобализации, так и развитием информационных технологий. В настоящее время киберпреступления являются самыми быстрорастущими уголовными преступлениями по сравнению с другими.

По данным Академии управления при Президенте Республики Беларусь, в нашей стране в период 2015–2020 гг. наблюдался устойчивый рост количества регистрируемых киберпреступлений. При этом, как сообщает заместитель председателя Следственного комитета Республики Беларусь Анатолий Васильев, за первый квартал 2022 г. зарегистрировано всего 2833 инцидента [1]. Это говорит о снижении числа преступлений в сфере информационных технологий.

Известно, что криминалистическая характеристика преступлений – это система криминально значимой информации о типичных, связанных элементах определенных категорий преступлений и условиях их совершения. Структура понятия криминалистической характеристики по своему смысловому наполнению совпадает с понятием криминалистической структуры преступления. Это утверждение не бесспорно, потому что рассматриваемые термины имеют разное смысловое значение.

Криминалистическая характеристика преступлений в сфере компьютерной безопасности представляет собой систему информации, полученной в результате специальных научных исследований, которая является основным структурным элементом методологии расследования этих преступлений и способствует их выявлению, расследованию и предотвращению.

Преступления, предусмотренные в главе 31 Уголовного кодекса (далее – УК) Республики Беларусь «Преступления против информационной безопасности», можно называть компьютерными. При этом понятие «компьютерные преступления» шире, чем «преступления против инфор-

мационной безопасности». Так, с криминалистической точки зрения с использованием компьютера как орудия или средства совершения преступления можно осуществить и шпионаж, и мошенничество, и подлог документов, и фальшивомонетничество, и злоупотребление служебными полномочиями, и многие другие преступления самыми различными способами.

Говоря о криминалистической характеристике преступлений в сфере информационной безопасности, следует отметить, что анализ научных источников свидетельствует также о существовании позиции, согласно которой в зависимости от уровня сведений, содержащихся в криминалистической характеристике, различают три ее уровня: общую криминалистическую характеристику преступлений (характеристику всех видов преступлений); видовую криминалистическую характеристику преступлений; индивидуальную криминалистическую характеристику конкретного преступления [5, с. 34–44]. Киберпреступления относятся ко второму уровню, а именно к видовой криминалистической характеристике. Видовая криминалистическая характеристика – это определенная система описания криминалистических значимых признаков, которые проявляются в особенностях способа, механизма и среды для подготовки, совершения и сокрытия преступления. Данная характеристика дает представление о самом преступном вмешательстве, субъекте, потерпевшем и других обстоятельствах преступления, которые являются методическим обеспечением успешного решения задач выявления, раскрытия, расследования и предотвращения преступлений выбранного типа.

Значительное воздействие на распространенность киберпреступлений оказывают и социально-психологические условия. В киберпреступной среде значительно претерпевает изменение психологическая сущность связей «преступник – предмет преступления», «преступник – потерпевший», которые из прямых превращаются в косвенную «преступник – электронное устройство – потерпевший», что приводит к отсутствию материальной (физической) составляющей как деяний лица, так и общественного взаимодействия. «Виртуализация» вреда обусловливает своеобразное понимание его жертвой преступления. Так, жертва, выявляя нанесенный ей «нефизический» или иной вред, не полно понимает его характер и масштабы, а значит, и характер, и степень общественной опасности содеянного в отношении ее деяния. Так же жертва не может правильно оценить взаимосвязь нанесенного вреда с каким-либо определенным преступником. В итоге произошедшее в отношении ее противоправное опасное деяние и нанесенный им ущерб жертвой зачастую оценивается как «зло», которое не может быть компенсировано.

Изучение уголовных дел и существующие теоретические концепции криминалистической характеристики преступлений позволяют определить ее содержание, в которое необходимо включить следующие структурные элементы:

– предмет преступного посягательства;

– типичные способы совершения и сокрытия преступления;

– следовую картину;

– типичные сведения о личности преступника, мотивах и целях общественно опасного поведения;

– данные о личности потерпевшего;

– закономерные связи между ними.

В зависимости от сообразительности, интеллектуальности преступника, в ряде случаев невозможно привести исчерпывающий перечень способов совершения преступлений в сфере преступлений против информационной безопасности, поскольку их содержание могут составлять самые разнообразные действия.

Говоря о месте совершения преступления, следует отметить, что место совершения общественно опасного правонарушения обычно не совпадает с местом, где имеют место реальные опасные последствия. Таких мест может быть несколько. Тщательный осмотр позволяет выявить следы субъекта, его знакомство с обстановкой и, возможно, с потерпевшим. При удаленном доступе место совершения преступления и место наступления последствий, как правило, различаются.

Говоря об обстановке при совершении преступлений в сфере компьютерной информации, следует отметить, что для нее характерно несоответствие места совершения правонарушения месту возникновения общественно опасных последствий. Преступления в информационной сфере совершаются с помощью специальной техники и оборудования.

Субъекты информационных преступлений обычно обладают специальными навыками и знаниями в области обработки информации в информационных системах. В качестве следовоспринимающего элемента субъект можно рассматривать по отношению только к средству совершения преступления. Следы, которые отразились на объекте преступного посягательства от иных структурных элементов преступления, образуют следовую картину, сведения о которой являются элементом криминалистической характеристики. Делая вывод об исследовании следовой картины при совершении преступлений против информационной безопасности, следует отметить, что в качестве следов могут выступать: 1) следы уничтожения информации; 2) следы доступа с помощью локальных сетей; 3) изменение первичной информации на различных носителях.

Часто субъекты данных преступлений являются людьми с высоким уровнем интеллекта, фанатичным подходом к новым компьютерным технологиям, смекалкой, с богатой фантазией и скрытностью. Если данные преступления совершены определенными группировками, то для таких формирований характерны четкое разделение ролей, корыстные мотивы и продуманная система сокрытия следов.

Мотивы и цели совершения преступлений различны (например, корысть, месть, хулиганские побуждения и озорство, исследовательские цели, демонстрация личных интеллектуальных способностей или превосходства). Причиной криминализации в белорусском уголовном законодательстве противоправных действий в области электронной техники и информационных технологий является их высокая общественная опасность.

Таким образом, криминалистическая характеристика преступлений против информационной безопасности имеет определенные особенности, которые следует учитывать при формировании методики расследования таких преступлений. Это прежде всего специфические средства и способы совершения преступных посягательств, а также определенные условия и факторы, способствующие совершению преступлений.

Кроме того, необходимо принимать во внимание и отличительные черты личности, которая совершает преступления против информационной безопасности. Выделение элементов криминалистической структуры преступлений против информационной безопасности, а также анализ обеспечивают наиболее полное и объективное познание конкретного преступления. При изучении следовой картины выявляется связь между способом совершения преступления, свойствами субъекта посягательства и обстановкой, в которой совершено преступное деяние данным способом.

Появление новых технических и программных средств, а также усложнение схем и способов совершения преступлений, изменение законодательства в данной сфере, разработка и внедрение цифровой экономики в Республике Беларусь позволяют также говорить о необходимости совершенствования методики расследования данной группы преступлений. Необходима систематизация всех достижений криминалистики, переоценка с учетом реалий сегодняшнего дня. Исходя из этого, следователь при определении направления расследования преступления должен учитывать и опираться на систему сведений, которые составляют криминалистическую характеристику рассматриваемого преступления, что позволит оптимизировать процесс расследования.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Киберпреступность в Беларуси [Электронный ресурс] // БелТА: Инфографика. – Режим доступа: https://www.belta.by/infographica/view/kiberprestupnost-v-belarusi-24963/.

2. Число киберпреступлений снизилось почти вдвое. Зампред СК о тенденциях в области IT-преступлений [Электронный ресурс] // БелТА: Общество. – Режим доступа: https://www.belta.by/society/view/chislo-kiberprestuplenij-snizilos-pochti-vdvoe-zampred-sk-o-tendentsijah-v-oblasti-it-prestuplenij-496880-2022/.

3. Белкин, Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики / Р. С. Белкин. – М. : Инфра-М-НОРМА, 2001. – 240 с.

4. Белкин, Р. С. Курс криминалистики. В 3 т. Т. 3. Криминалистические средства. Приемы и рекомендации / Р. С. Белкин. – М. : Юристъ, 1997. – 658 с.

5. Густов, Г. А. Понятие и виды криминалистической характеристики преступлений / Г. А. Густов // Криминалистическая характеристика : сб. науч. тр. / под ред. В. В. Клочкова. – М., 1984.

К содержанию

УДК 343.1

И. А. ЗАРАНКА
Брест, БрГУ имени А. С. Пушкина

ПРАВОВЫЕ АСПЕКТЫ ИНСТИТУТА ДОПРОСА В РЕСПУБЛИКЕ БЕЛАРУСЬ

Допрос является наиболее распространенным следственным действием. Согласно исследованиям, в среднем около 66 % протокольных материалов уголовных дел составляют протоколы допросов. Следователи проводят около 25 % своего времени на допросах. Это объясняется высокой информационной емкостью каждого отдельного опроса, его гносеологическим значением.

Итак, сущность допроса состоит в востребовании от допрашиваемого показаний при помощи приемов криминалистической тактики, разработанных на основе обобщения следственной и судебной практики. Следовательно, допрос может быть определен как следственное и судебное действие, направленное на получение следственным органом или судом в соответствии с правилами, установленными процессуальным законом, информации, которая была допрошена или имеет большое значение для правильного разрешения вопроса.

С точки зрения уголовного процесса и криминалистики допрос является средством доказательства и процессом получения доказательств,