Хлус, А. М. Криминалистическая структура преступлений против информационной безопасности / А. М. Хлус // Информационная безопасность как составляющая национальной безопасности государства : материалы Междунар. науч.-практ. конф., Минск, 11–13 июля 2013 года : в 3 т. / Ин-т нац. безопасности Респ. Беларусь ; редкол. : С. Н. Князев (гл. ред.) [и др.]. – Минск, 2013. – Т. 2. – 332 с. – С. 282–286. (тезисы)

УДК 343.98

А.М. Хлус

КРИМИНАЛИСТИЧЕСКАЯ СТРУКТУРА ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для любого преступления характерно наличие определенного количества материальных элементов, без которых его совершение невозможно. Их взаимосвязь при осуществлении противоправной деятельности образует внутреннюю структуру и приводит к достижению преступного результата. Не являются исключением в этом аспекте преступления против информационной безопасности.

В содержании криминалистической структуры преступлений против информационной безопасности можно выделить следующие общие элементы: субъект и объект преступного посягательства, средство совершения преступления и предмет преступного посягательства.

В каждом конкретном преступлении количество материальных элементов преступной структуры может быть различным. В связи с этим различают полную, упрощенную и усложненную криминалистические структуры преступления [1, с. 74]. Для полной структуры характерно наличие трех элементов, например, субъект, объект и средство преступного посягательства. В упрощенной преступной структуре меньшее количество элементов и, соответственно, больше в усложненной, чем в полноструктурном преступлении. Анализ преступлений против информационной безопасности позволяет сделать вывод о наличии в их содержании полной либо усложненной криминалистической структуры.

В качестве субъекта преступленного посягательства всегда можно рассматривать только человека. В структуре преступлений против

информационной безопасности субъект проявляет себя преимущественно как следообразующий элемент.

Изучение результатов любого преступления против информационной безопасности позволяет выявить следы, содержащие сведения о личности преступника, его социально-психологических свойствах, профессиональных качествах, опыте, специальных знаниях, возрасте и т.д.

Объектом преступного посягательства является компьютерная система, сети или машинные носители информации.

Средством совершения преступления являются компьютерная техника, программные (аппаратные) средства, обеспечивающие доступ к защищенной компьютерной системе или сети, вредоносные программы.

Предметом преступного посягательства являются компьютерная информация (программа). В качестве предмета может выступать также компьютерное оборудование, компьютерная система, сеть или машинный носитель информации.

Выделение элементов криминалистической 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, сведения о которой являются элементом криминалистической характеристики [2, с. 237]. Анализ специфики формирования следовой картины при совершении преступлений против

информационной безопасности 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 [2, с. 247]. Нетрадиционный характер этих следов привел к предложению ввести понятие «виртуальный след», под которым понимается «зафиксированный компьютерной системой на цифровом материальном носителе результат отражения реального физического процесса или действия иной компьютерной системы, связанный с преступлением (имеющий уголовно-релевантное значение), в виде цифрового образа формальной (математической) модели этого процесса» [3, 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 против информационной безопасности. Их использование при исследовании объекта преступного посягательства позволяет следователю выдвинуть наиболее вероятную версию о субъекте преступного посягательства.

Для установления субъекта преступного посягательства интерес представляет обобщенная информация, содержащаяся в криминалистической характеристике преступлений против информационной безопасности. Согласно данной характеристике все субъекты с учетом способа совершения преступлений разделены на две группы. Первую составляют лица, для которых характерным мотивом преступных действий является профессиональная самореализация в сфере компьютерных технологий. Вторую группу составляют лица, у которых преобладает корыстная направленность при различном уровне владения навыками в сфере компьютерных технологий.

Первую группу образуют так называемые хакеры, крэкеры, вирмейкеры. Во вторую группу входят кардеры, фрикеры, компьютерные пираты.

Для хакеров характерно использование способов, которые направлены на демонстрацию профессионального мастерства и обеспечивают несанкционированный доступ к информации в компьютерной системе, сети или на машинном носителе. При этом возможно ее копирование без цели использования.

Целью крэкера является не только взлом компьютерной системы несанкционированный доступ к информации, но и ее кража, подмена, блокирование или уничтожение.

Деятельность вирмейкеров связана с использованием и разработкой вирусных и вредоносных программ, а также в ряде случаев с получением несанкционированного доступа.

Преступная деятельность кардеров направлена на завладение чужими вещами или деньгами. В связи с этим различают вещевой и денежный кардинг. Основой для совершения этих преступлений являются чужие кредитные карты. Действия кардеров, в первую очередь, направлены на несанкционированное получение информации о держателе карты. Это позволяет в дальнейшем заказать товары в интернет-магазинах или изготовить поддельные кредитные карты.

Фрикеры используют телефонные системы для целей уклонения от оплаты телекоммуникационных услуг.

Компьютерные пираты используют способы, связанные со взломом программного обеспечения, с целью удаления предусмотренного разработчиком системы защиты от несанкционированного копирования и тиражирования [2, с. 238].

На основе выше изложенного можно сделать некоторые выводы.

Во-первых, расследование преступлений против информационной безопасности должно осуществляться на основе познания их структурных элементов. В криминалистической структуре данного вида преступлений

следующие общие элементы: субъект и объект преступного посягательства, средство совершения преступления и предмет преступного посягательства.

Во-вторых, эффективность познания отдельных элементов преступной структуры увеличивается при условии использования знаний, содержащихся в криминалистической характеристике преступлений против информационной безопасности.

Литература:

1. Гучок, А.Е. Криминалистическая структура преступлений / А.Е. Гучок. - Минск: БГУ. – 2007. – 151 с.

2. 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.

3. 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. – 267 с.