В обобщенном виде подход зарубежного законодательства выглядит так, что, с одной стороны, электронные деньги представляют собой особые средства обращения традиционных и частных валют, которые используются для упрощения финансовых расчетов при оплате товаров и услуг в сети Интернет, с другой – обязательства эмитента, которые исполняются в традиционных, не электронных деньгах [2, с. 96–97].

Сеть Интернет представляет собой всемирную информационную компьютерную сеть, именуемую в повседневном общении – мировой паутиной. Она аккумулирует огромное количество компьютерных сетей, работающих по единым правилам, и включает пользователей почти из всех стран мира. Однако единство правил относится в значительной степени к технической составляющей, чем к правовой, поскольку по целому ряду правовых вопросов нет международного единства мнений. В связи с этим перед лицами, производящими дознание в ОПС, стоит задача: производить дознание по преступлениям, создающим угрозу пограничной безопасности, совершенным с использованием сети Интернет, опираясь на национальное законодательство, но в рамках международного взаимодействия учитывать и законодательство страны, с которой необходимо осуществлять международное сотрудничество, направленное на фиксацию доказательств в рамках расследования уголовного дела. Анализ уголовных дел по преступлениям данной категории свидетельствует о том, что преступления имеют межрегиональный и международный характер, что также негативно сказывается на результатах расследования уголовных дел по причине «запаздывания» производства следственных действий и их фиксации. При фиксации доказательственной информации, хранящейся на ресурсах сети Интернет, лицу, производящему дознание, необходимо учитывать уголовно-процессуальные нормы, общие криминалистические рекомендации, технические особенности работы компьютерных систем и сетевого интернет-пространства.

Фиксация доказательственной информации, содержащей цифровые следы, должна быть представлена в виде последовательной и полной цепи отраженных в процессуальных документах сведений, замкнутых по смыслу. В качестве таких процессуальных документов целесообразно рассматривать протоколы осмотра смартфонов, ноутбуков и других гаджетов.

В современный период при совершении преступлений, создающих угрозу пограничной безопасности, в первую очередь организация незаконной миграции, незаконное перемещение через таможенную границу Евразийского экономического союза и (или) Государственную границу Республики Беларусь наркотических средств, психотропных веществ

либо их прекурсоров или аналогов и других, лицами, совершающими данные преступные деяния, активно используются современные информационные технологии, позволяющие скрывать личность, а также следы совершаемых преступлений. Вместе с тем развитие криминалистической техники и тактики позволяет обнаруживать и фиксировать цифровые следы, которые остаются в данном случае. Вышеизложенное обусловливает активное использование лицами, производящими дознание в ОПС, положений нового раздела криминалистической техники, как «форензика» для решения задач при расследовании преступлений.

При расследовании преступлений, создающих угрозу пограничной безопасности, при совершении которых используются информационные технологии, чаще используется проведение такого следственного действия, как осмотр смартфонов, ноутбуков и других гаджетов. В процессе его осуществления с большой вероятностью может быть осуществлено обнаружение цифровых следов, с последующей их фиксацией, изъятием и использованием при расследовании по уголовным делам. Фиксация содержания цифровых следов предполагает отображение последовательной и полной цепи ее отражения в виде сведений, замкнутых по смыслу, в таких процессуальных документах, как протоколы осмотра смартфонов, ноутбуков и других гаджетов.

1. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : в ред. Закона Респ. Беларусь от 13.05.2022 г. № 165-З // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

2. Колычева, А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети интернет : автореф. дис. ... канд. юрид. наук : 12.00.12 / А.Н. Колычева ; Рос. гос. ун-т правосудия. – М., 2018. – 199 с.

УДК 343.985.7

Ю.М. Юбко

ОБСТОЯТЕЛЬСТВА, ПОДЛЕЖАЩИЕ ДОКАЗЫВАНИЮ ПО МАТЕРИАЛАМ И УГОЛОВНЫМ ДЕЛАМ О ПРЕСТУПЛЕНИЯХ ПРОТИВ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Процессуально закрепленные следы являются носителями информации, позволяющей установить обстоятельства, подлежащие доказыванию в соответствии с требованиями ст. 89 и 90 Уголовно-процессуального кодекса Республики Беларусь (УПК), так как данные нормы явля-

ются общими, то следователь (лицо, производящее дознание) обязан учитывать особенности конструкции ст. 349–355 Уголовного кодекса Республики Беларусь (УК). При этом все обстоятельства (ст. 89 УПК) должны быть достоверно установлены совокупностью доказательств.

Обстоятельства, подлежащие доказыванию применительно к рассматриваемым преступлениям, могут быть условно подразделены на две группы: общие и частные.

Почти для всех преступлений гл. 31 УК относительно доказывания «наличие общественно опасного деяния…» (п. 1 ч. 1 ст. 89 УПК) общим является предмет преступного посягательства – компьютерная информация, хранящаяся в компьютерной системе, сети или на машинных носителях, а также – носители этой информации: компьютерное оборудование, компьютерная система, сеть, машинные носители, компьютерные программы и т. п. Однако в случае совершения деяния, предусмотренного ст. 354 УК, о предмете преступного посягательства следует вести речь как о частном «обстоятельстве», так как в конструкции нормы законодатель говорит о вредоносных компьютерных программах или специальных программных или аппаратных средствах.

Проводя разграничение по другим признакам, характеризующим общественно опасное деяние как преступление против компьютерной безопасности, следует подчеркнуть, что могут иметь место как общие, так и в отдельных случаях частные особенности, характеризующие отдельные элементы способа, а в ряде ситуаций и их совокупность (пробные попытки вхождения в информационную сеть или систему; подбор пароля; использование вредоносных компьютерных программ; использование чужого имени (пароля); маскировка под законного пользователя и т. п.). Данные элементы способа характерны для преступных действий, предусмотренных ст. 349, 350, 352 УК.

Относительно доказывания элементов способа совершения преступлений, предусмотренных ст. 354, 355 УК, необходимо вести речь о группе частных обстоятельств, так как в уголовно-правовой конструкции имеются особенности в предмете преступного посягательства (ст. 354 УК) и в субъекте преступления (ст. 355 УК).

Применительно к конструкции ст. 354 УК, следует доказать одно (или совокупность) действие, осуществляемое субъектом с предметом преступления, – разработка; использование; распространение; сбыт компьютерной программы или специального программного или аппаратного средства [1, с. 178–180], заведомо предназначенных для нарушения системы защиты, несанкционированного доступа к компьютерной системе, сети или машинному носителю, несанкционированного уничтожения, блокирования, модификации компьютерной информации или

неправомерного завладения компьютерной информацией либо нарушения работы компьютерной системы, сети или машинного носителя.

В ч. 1 ст. 355 УК законодатель констатирует, что субъектом преступления является лицо, имеющее доступ к компьютерной системе или сети, т. е. лицо, являющееся законным пользователем. С учетом этого способ совершения имеет частные особенности, обусловленные правами пользователя. Принимая во внимание отмеченное, должно быть доказано, что лицо совершило преступные действия путем нарушения (игнорирования) технических правил или запретов, установленных собственником (владельцем) системы или сети, которые повлекли наступление существенного вреда, выразившегося в причинении ущерба собственнику, владельцу, пользователю или третьим лицам (например, клиентам электронных платежных систем и т. п.).

Доказывание «места совершения преступления против компьютерной безопасности» обусловлено установлением как общих, так и частных обстоятельств: во-первых, связанных с подготовкой и началом совершения преступных действий в законном владении субъекта, учреждении или организации любой формы собственности, и т. п.; во-вторых, связанных с совершением преступных действий как на территории Республики Беларусь, так и за ее пределами; в-третьих, связанных с использованием подозреваемым существующих телекоммуникационных и компьютерных сетей. Понятие «место совершения преступления против компьютерной безопасности» содержит в своем смысловом выражении не только дефиницию «место подготовки и совершения данного вида преступления», но и «место наступления вредных последствий», т. е. конкретное юридическое или физическое лицо, которым причиняется преступными действиями вред (место фактического их нахождения).

Исследуя обстоятельства, подлежащие доказыванию, необходимо остановиться на рассмотрении такого из них, как орудие совершения преступления. В общедоступном понимании по делам рассматриваемой категории к «орудиям совершения преступления» следует отнести программно-технические средства (средства компьютерной техники (СКТ); программное обеспечение). Под термином программно-технические средства, следует понимать не только СКТ и различное программное обеспечение (вредоносные компьютерные программы и т. п.), а также технические средства, функциональные возможности которых позволяют получить доступ к информационной системе и (или) информационной сети для совершения преступления.

Пункт 2 ч. 1 ст. 89 УПК обязывает при производстве предварительного следствия доказывать виновность обвиняемого в совершении преступления, в связи с чем необходимо исследовать личность субъекта и субъективную

сторону совершенного преступления. Применительно к рассматриваемым деяниям субъектом является физическое вменяемое лицо, достигшее 16 лет. Однако в конструкции ст. 355 УК законодатель ведет речь о специальном субъекте – лице, имеющем доступ к компьютерной системе или сети.

При исследовании субъективной стороны должен быть доказан характер вины обвиняемого, т. е. совершено деяние умышленно или по неосторожности. Преступления, предусмотренные ч. 1 и 2 ст. 349, ч. 2 ст. 350, ст. 355 УК, являются неосторожными, ст. 354 УК предусматривает умышленное преступление. Совершение же деяний, указанных в ч. 1 ст. 350 и ст. 352 УК, возможно как умышленно, так и по неосторожности. При обвинении лица в совершении умышленного преступления необходимо доказать содержание умысла – мотив, цель, а при обвинении в неосторожном преступлении – в чем конкретно выразилась неосторожность. По некоторым деяниям мотив является необходимым признаком состава преступления, а по другим – он может быть обстоятельством, смягчающим или отягчающим ответственность. Цель совершения преступления устанавливается исходя из всей совокупности обстоятельств, характеризующих действия лица, включая подготовительные действия, способы и орудия преступления [2, с. 244–245].

В ч. 2 ст. 350, 352, 354 УК законодатель выделяет квалифицирующий признак «…совершенных группой лиц», поэтому, когда данные преступления совершены в соучастии, должны быть установлены все члены преступной группы, роль и степень индивидуального участия каждого из них.

Доказывание характера и размера вреда, причиненного рассматриваемыми деяниями, представляет собой довольно сложную задачу, так как вред редко выражается в виде прямых убытков [3, с. 122]. Используемые законодателем в нормах УК в этой связи отдельные термины носят оценочный характер. Так, «существенный вред» может выражаться в виде причиненного материального ущерба в одних ситуациях, а в других – он проявляется в виде создания препятствий для нормального функционирования государственных органов и иных организаций или нарушения конституционных прав граждан Республики Беларусь. Вместе с тем независимо от возникающих сложностей в практической деятельности при разрешении данного вопроса представляется, что характер и размер вреда необходимо определять в зависимости от квалификации преступных действий субъекта с учетом формирования его преступного умысла, цели, наступления вредных последствий в рамках процессуальной формы, определенной законодателем в гл. 17 УПК. Основополагающим критерием при этом является требование ч. 1 ст. 148 УПК о том, что преступлением причинен физический, имущественный или моральный вред.

Представляется целесообразным обратить внимание также на круг обстоятельств, подлежащих установлению в стадии возбуждения уголовного дела. В стадии возбуждения уголовного дела орган уголовного преследования устанавливает наличие или отсутствие достаточных данных, указывающих на признаки преступлений, предусмотренных гл. 31 УК. Если решение о возбуждении уголовного дела принимается органом дознания, то производство неотложных следственных и иных процессуальных действий направлено на установление и закрепление следов преступлений против компьютерной безопасности.

1. Уголовный кодекс Республики Беларусь : науч.-практ. коммент. / Т.П. Афонченко [и др.] ; под ред. В.М. Хомича, А.В. Баркова, В.В. Марчука. – Минск : Нац. центр правовой информ. Респ. Беларусь, 2019. – 1000 с.

2. Научно-практический комментарий к Уголовно-процессуальному кодексу Республики Беларусь / Н.И. Андрейчик [и др.] ; под науч. ред. М.А. Шостака ; учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь». – Минск : Акад. МВД, 2014. – 1230 с.

3. Организация расследования преступлений в сфере высоких технологий : учеб. пособие / П.В. Гридюшко [и др.] ; под общ. ред. И.Г. Мухина ; учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь». – Минск : Акад. МВД, 2017. – 139 с.

УДК 343.9

Н.В. Якимович

ПОНЯТИЕ КРИМИНАЛИСТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ВЫЯВЛЕНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В последние годы проблемам раскрытия и расследования преступлений, совершаемых с использованием информационных технологий, было уделено определенное внимание в монографиях, учебных пособиях и научных статьях отечественных авторов. Однако большая их часть посвящена в основном исследованию уголовно-правовых и криминологических аспектов, в то время как криминалистические аспекты указанной проблемы изучены в меньшей степени.

Под преступлениями, совершаемыми с использованием информационных технологий, мы будем понимать преступления в сфере компьютерной безопасности (гл. 31 Уголовного кодекса Республики Беларусь), которые в большинстве случаев являются предикатными для со-