В этой связи предлагается исходить из опыта зарубежных государств и признавать действия провокационными или считать их совершенными в рамках правомерного оперативного эксперимента в зависимости от степени понуждения к получению взятки с целью последующего изобличения. При оценке таких действий, как проведение оперативного эксперимента, следует исходить из следующих обстоятельств: 1) до проведения оперативного эксперимента уже была доказана предрасположенность к такому поведению у должностного лица и степень склонения была незначительной; 2) воздействие сотрудничающего лица с целью понудить должностное лицо взять взятку не являлось дискредитирующим правовые и нравственные принципы поведением. В то же время провокационными действиями признается такое поведение, когда: 1) преступный умысел взяткополучателя был всецело инициирован сотрудничающим лицом; 2) воздействие с целью понудить должностное лицо взять взятку являлось поведением, дискредитирующим правовые и нравственные принципы.

Оперативный эксперимент является правомерным, реально осуществимым и эффективным ОРМ по выявлению и раскрытию дачи-получения взяток. Как показывает изученная нами следственная практика, информация, полученная в результате проведения данного ОРМ, активно используется на стадии предварительного расследования и направлена на изобличение взяточников. Вместе с тем для обеспечения возможности использования результатов оперативного эксперимента при расследовании уголовных дел о взяточничестве необходимо соблюдение законности при его осуществлении. К одному из таких требований законности относится недопущение совершения провокационных и инсценированных действий со стороны лиц, участвующих в оперативном эксперименте.

Д.Н. Лабоцкий, *старший следователь по особо важным делам СУ ПР УВД Гродненского облисполкома, аспирант ГрГУ им. Я. Купалы*

ПРЕСТУПЛЕНИЯ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

До недавнего времени считалось, что преступления против информационной безопасности не присущи Республике Беларусь по причине слабой компьютеризации нашего общества, недостаточного внедрения в производственные и общественные отношения информационных технологий. Только сейчас проблема борьбы с преступлениями против информационной безопасности начала рассматриваться в уголовно-правовом аспекте, когда материальные потери от этого вида преступлений достигли существенных размеров. Россия первая из стран СССР официально заявила о проблемах борьбы с преступлениями против информационной безопасности (в июле 1992 г. с момента создания постоянно действующего межведомственного семинара «Криминалистика и компьютерная преступность», организованного в рамках координационного бюро по криминалистике при НИИ проблем укрепления законности и правопорядка Генеральной прокуратуры Российской Федерации и Экспертно-криминалистического центра МВД России).

Общественная опасность преступных действий в сфере высоких технологий становится очевидной. В Республике Беларусь при всех УВД облисполкомов уже созданы отделы по раскрытию преступлений в сфере высоких технологий, основными целями которых являются: выявление и раскрытие преступлений в сфере компьютерной информации и телекоммуникаций (высоких технологий); борьба с незаконным оборотом радиоэлектронных и специальных технических средств, пресечение изготовления, распространения и использования на территории Беларуси несертифицированной (запрещенной для использования) радиотехники и аппаратуры; проведение аналитической (информационной) и компьютерной разведки с целью поиска криминальной и иной информации, представляющей оперативный интерес, циркулирующей в радиотехнических и информационных сетях, и т. д.

«Первым человеком, применившим ЭВМ для совершения налогового преступления на сумму 620 тыс. долларов и в 1969 г. представшим за это перед американским судом, стал Альфонсе Конфессоре. Дальнейшая история преступлений, где средством совершения является компьютер или объектом выступает информация, отмечена такими наиболее "яркими" событиями: конец 70-х – "ограбление" "Секьюрити пасифик банк" (10,2 млн долларов); 1979 г. – компьютерное хищение в Вильнюсе (78 584 р.); 1984 г. – сообщение о первом в мире "компьютерном вирусе"; 1985 г. – вывод из строя

при помощи "вируса" электронной системы голосования в конгрессе США; 1987–1988 гг. – появление первого "компьютерного вируса" в СССР; 1989 г. – блокировка американским студентом 6000 ЭВМ Пентагона; международный съезд компьютерных "пиратов" в Голландии с демонстрацией возможности неограниченного внедрения в системы ЭВМ; 1991 г. – хищение во Внешэкономбанке на сумму в 125,5 тыс. долларов; 1992 г. – умышленное нарушение работы АСУ реакторов Игналинской АЭС; 1993 г. – неоконченное электронное мошенничество в Центробанке России (68 млрд р.); 1995 г. – попытка российского инженера украсть из Сити-банка 2,8 млн. долларов»[1].

Компьютерная преступность становится одним из наиболее опасных видов преступных посягательств. «По данным ООН, уже сегодня ущерб, наносимый компьютерными преступлениями, сопоставим с доходами от незаконного оборота наркотиков и оружия. Только в США ежегодный экономический ущерб от такого рода преступлений составляет около 100 миллиардов долларов. Причем многие потери не обнаруживаются или о них не сообщают»[2].

Говоря о понятии «компьютерные преступления», необходимо отметить, что данный термин используется в зарубежных правоохранительных органах с 1990-х гг. и подразумевает преступления, связанные с использованием компьютера. Однако понятия «компьютерные преступления» и «компьютерная преступность» охватывают все преступления, совершаемые при помощи компьютера, и являются более широкими понятиями, чем «преступления против информационной безопасности». С точки зрения В.Б. Вехова, «…компьютерные преступления с криминалистической точки зрения нужно рассматривать как предусмотренные уголовным законом общественно опасные действия, совершенные с использованием средств электронно-вычислительной техники»[3]. По мнению многих ученых, в том числе и В.А. Мещерякова, «…под компьютерными преступлениями следует понимать предусмотренное уголовным законом общественно опасное деяние (действие или бездействие), направленное против информации, представленной в особом (машинном) виде, принадлежащей государству, юридическому или физическому лицу, а также против установленного государством или его собственником порядка создания (приобретения), использования и уничтожения, если оно причинило или представляло реальную угрозу причинения ущерба законному владельцу информации или автоматизированной системы, в которой эта информация генерируется (создается), обрабатывается, передается или уничтожается или повлекло иные опасные последствия»[4]. Уголовный кодекс Республики Беларусь предусматривает наказание за преступления в сфере компьютерной информации, где информация и информационные отношения являются объектом преступления.

В настоящее время в юридической науке нет однозначного определения объекта преступления против информационной безопасности, как и определения самого преступления в сфере компьютерной информации. Одна часть исследователей относит к компьютерным преступлениям действия, в которых компьютер является либо объектом, либо орудием посягательства. При этом кража самих компьютеров рассматривается как один из способов совершения компьютерных преступлений. Другие исследователи относят к компьютерным преступлениям только противозаконные действия в сфере автоматизированной обработки информации. В этом случае объектом посягательства является информация, обрабатываемая в компьютерной системе, а компьютер служит орудием посягательства, хотя правильным было бы называть их преступлениями против информационной безопасности. Отметим, что законодательство многих стран, в том числе России и Беларуси, стало развиваться именно по этому пути. Ошибочно похищение аппаратной структуры компьютера считать компьютерным преступлением, поскольку, хотя посягательство и направлено на компьютер как на предмет, оно нарушает отношение собственности, а не информационную безопасность и должно квалифицироваться как преступление против собственности. Правильно отмечает Н.Ф. Ахраменка, что «…сам компьютер не может быть рассмотрен как предмет преступлений против информационной безопасности, так как предметом посягательств при их совершении является отнюдь не техника как таковая, а информация, хранимая, обрабатываемая или передаваемая этой техникой»[5]. Согласно ст. 1 соглашения «О сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» под преступлением в сфере компьютерной информации следует понимать уголовно наказуемое деяние, предметом которого является компьютерная инфор-

[1] Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 8.

[2] Волеводз А.Г. Противодействие компьютерным преступлениям. М.: Юрлитинформ, 2002. С. 20.

[3] Вехов В.Б. Компьютерные преступления. Способы совершения и раскрытия. М., 1996. С. 24.

[4] Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. Воронеж: Воронеж. гос. ун-т, 2001. С. 44.

[5] Вопросы квалификации, регистрации и учета преступлений / Под общ. ред. А.И. Лукашова. Минск: Акад. МВД Респ. Беларусь, 2003. С. 37.

мация, находящаяся в памяти компьютера, на машинных носителях, в форме, доступной для восприятия ЭВМ, или передающаяся по каналам связи.

Впервые ученые обратились к разработке проблемы борьбы с преступлениями против информационной безопасности в конце 1980-х гг. Уже в начале 90-х гг. зарубежные правоохранительные органы повсеместно столкнулись с преступлениями, связанными с использованием компьютера. Данный вид стал новой формой международной преступности. С середины 90-х гг. к данной проблеме обратились и российские ученые. Ю.М. Батурин, А.М. Жодзинский, Н. Селиванов, А. Комиссаров впервые на постсоветском пространстве в криминалистике подняли проблему преступлений против информационной безопасности, называя их компьютерными преступлениями, рассмотрели понятие, криминологические аспекты и способы совершения данных преступлений. Объектом преступного посягательства в преступлениях против информационной безопасности является информация, а действия преступника следует рассматривать как покушение на информационные отношения общества.

Значение компьютерной криминалистической информации для раскрытия и расследования уголовных преступлений велико. Оно очевидно даже при перечислении основных видов сведений, которые пользователи вводят, хранят, обрабатывают и которыми обмениваются с другими юридическими и физическими лицами с помощью компьютерной техники. Если для раскрытия преступления достаточно общих сведений о той компьютерной информации, которой располагают заподозренные физические и юридические лица, то значительно более важной и сложной является задача изъятия этой информации и рассмотрения ее с точки зрения доказывания по уголовному делу. Наличие на компьютерах, в системах и сетях большого объема информации показывает, что следователь должен четко представлять, какие именно фактические данные он может получить с помощью ЭВМ, каково их доказательственное значение и способы введения в уголовное дело в качестве доказательств. До настоящего времени законодатель однозначно не выразил отношения к информации, хранящейся в памяти компьютера, как к доказательству. Сегодня назрела необходимость единообразного понимания и использования компьютерной информации.

На сегодняшний день правоохранительные органы не располагают достаточным количеством разбирающихся в современной технике специалистов, способных оперативно выявлять и расследовать компьютерные преступления, поэтому создание целостной системы обучения, подготовки и переподготовки специалистов по борьбе с информационными правонарушениями является одной из основных задач. Следует особо подчеркнуть, что процессы эффективного выявления, расследования и проведения экспертиз компьютерных правонарушений требуют создания всех необходимых для этого методических и технических средств. Ввиду слабой разработанности соответствующего инструментария данная задача становится первостепенной при реализации мер по адекватному противодействию преступлениям в сфере компьютерной информации. С указанным направлением тесно связана проблема совершенствования нормативно-правовой базы, недостаточная развитость которой пока не позволяет в должной мере противостоять криминальным действиям в сфере компьютерной информации. Уголовные санкции на национальном и международном уровнях еще не обеспечивают надежной защиты от компьютерной преступности по следующим причинам: из-за отсутствия в существующих законах четкой классификации компьютерных преступлений и сложности толкования и применения статей законов, ограничивающих действия правоохранительных органов. Более того, несмотря на введение в Уголовный кодекс Республики Беларусь составов преступлений против информационной безопасности, устоявшийся понятийный аппарат относительно указанного вида деяний еще не сложился. Уголовные законы пока не подкреплены соответствующими гражданскими санкциями.

Для построения национальной системы борьбы с правонарушениями в сфере компьютерной информации необходимо провести комплекс научно-исследовательских и опытно-конструкторских работ по совершенствованию и созданию новых отечественных программных, программно-аппаратных и технических средств, обеспечивающих эффективную защиту компьютеров, компьютерных сетей от несанкционированного доступа, распространения вредоносных программ и т. д.

В настоящее время перед правоохранительными органами при расследовании преступлений против информационной безопасности возникают криминалистические проблемы, характеризующие одновременно и специфику этого процесса, а именно:

1) сложность в установлении факта совершения компьютерного преступления и решении вопроса о возбуждении уголовного дела;

2) сложность подготовки и проведения отдельных следственных действий;

3) особенности выбора и назначения необходимых экспертиз;

4) целесообразность использования средств компьютерной техники в расследовании преступлений данной категории;

5) отсутствие методики расследования преступлений против информационной безопасности.

По оценкам отечественных и зарубежных исследователей, решение проблем раскрытия и расследования преступлений данного вида представляет собой задачу на несколько порядков сложнее, чем задачи, сопряженные с их предупреждением. «Именно корыстный мотив по соотношению с другими мотивами преступлений в сфере компьютерной информации составляет 66 процентов»[1], поэтому «…уровень латентности компьютерных преступлений определяется в настоящее время в 90 процентов. А из оставшихся 10 процентов выявленных компьютерных преступлений раскрывается только лишь один»[2].

Решением проблемы является выработка единых следственных действий, обязательных при расследований преступлений против информационной безопасности (на основе анализа и систематизации способов совершения преступлений против информационной безопасности с учетом комплексного исследования различных мнений в зарубежной литературе, складывающейся практики при расследовании данных видов преступлений). Важность таких исследований состоит в следующем:

данный вид преступления в рамках правового поля Республики Беларусь существует чуть более пяти лет;

отсутствуют систематизированные рекомендации по расследованию преступлений против информационной безопасности;

нет единого технологического и алгоритмизированного подхода к рассматриваемой проблеме;

в существующих литературных источниках можно наблюдать противоречивость рекомендаций, разноплановость и отсутствие полноты вопросов и обстоятельств, подлежащих разрешению в процессе расследования уголовных дел по совершению преступлений против информационной безопасности;

в настоящее время возникла необходимость формирования единого сбалансированного блока криминалистических технологий по всем видам преступлений, предусмотренных гл. 31 УК Республики Беларусь;

целесообразно формирование и балансирование интегративно-тактических комплексов и алгоритмов, которые отражают общую характеристику каждого вида преступления против информационной безопасности;

актуально выделение алгоритма допроса по каждому виду преступления против информационной безопасности, чтобы раскрыть систему обстоятельств, подлежащих доказыванию по каждому составу преступления;

целесообразно сформировать специфическую интегрированную тактику отдельных следственных действий по делам против информационной безопасности.

Решение данных задач приведет к выработке конкретной тактики и методики расследования преступления против информационной безопасности.

А.П. Леонов, *профессор кафедры административной деятельности и управления органами внутренних дел Академии МВД Республики Беларусь, кандидат философских наук, доцент;*
Н.Е. Щербак, *преподаватель кафедры уголовного права, процесса и криминологии ЧУО «БИП – Институт правоведения»*

К ХАРАКТЕРИСТИКЕ ПРИЧИННОГО КОМПЛЕКСА КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

С учетом потребностей практики предупреждения компьютерной преступности характеристику ее причинного комплекса целесообразно рассмотреть, во-первых, в контексте особенностей процессов глобализации и информатизации общества и его основных сфер (экономической, политической, социальной, духовной), оказывающих влияние на формирование причин и условий компьютерной пре-

[1] Панов В.П. Сотрудничество государств в борьбе с международными уголовными преступлениями. М., 1993. С. 67.
[2] Вехов В.Б. Указ. соч. С. 44.