Д.А. Илюшин[*]

ОСОБЕННОСТИ ВОЗБУЖДЕНИЯ УГОЛОВНЫХ ДЕЛ О ПРЕСТУПЛЕНИЯХ, СОВЕРШАЕМЫХ В СФЕРЕ ПРЕДОСТАВЛЕНИЯ УСЛУГ «ИНТЕРНЕТ»

В статье автором подробно рассматриваются характерные поводы и основания возбуждения уголовных дел данной категории, предлагается алгоритм взаимодействия следователя с сотрудниками специализированного органа дознания (подразделений СТМ). Рассматриваются и иные вопросы, имеющие практическое значение для оптимизации процесса организации оперативно-служебной деятельности правоохранительных органов.

Как свидетельствует статистика, в последнее время количество преступлений, совершаемых в сфере предоставления услуг «Интернет» неуклонно увеличивается. Возрастает их удельный вес по размерам похищаемых сумм и другим видам ущерба в общей доле материальных потерь от противоправных проявлений. О динамике и масштабах этих преступных посягательств наглядно свидетельствуют следующие данные. За период с 1999 по 2004 гг. количество мошенничеств, совершенных в сети «Интернет», увеличилось в среднем в 2,5 раза и продолжает ежегодно увеличиваться в 1,5 раза. Одновременно с этим в 6,8 раз увеличилось количество фактов причинения имущественного ущерба пользователям «Интернет», посредством неправомерного использования принадлежащих им реквизитов доступа к сети. Общее количество зарегистрированных фактов неправомерного доступа к охраняемой законом компьютерной информации возросло в среднем в 38 раз[1].

С учетом изложенного представляется обоснованным вывод о том, что преступления рассматриваемой категории имеют высокую общественную опасность. Поэтому их выявление, раскрытие и расследование в современных условиях борьбы с преступностью являются приоритетной задачей, стоящей перед правоохранительными органами. Однако ее выполнение сопряжено со значительными трудностями. Это обусловлено рядом объективных и субъективных факторов, в числе которых можно выделить проблему отсутствия в отечественной криминалистике монографических работ, посвященных изучению особенностей возбуждения уголовных дел данной категории. Малоисследованным остается и вопрос организации взаимодействия подразделений предварительного следствия с органом дознания на этапе принятия указанного процессуального решения.

Илюшин Денис Анатольевич – заместитель начальника отдела Управления специальных технических мероприятий при ГУВД Самарской области

Исходя из результатов анализа материалов уголовных дел, основными путями выявления преступлений, связанных с предоставлением услуг «Интернет», являются следующие:

1) в ходе взаимодействия пользователей с компьютерной системой (при эксплуатации программного обеспечения, обмене информацией, использовании данных, проведении проверок и т.д.);

2) в результате проведения регулярных проверочных мероприятий сотрудниками службы безопасности или специалистами по защите информации, состоящими в штате пользователя или провайдера;

3) в ходе встреч оперативных сотрудников с лицами, оказывающим содействие органам, осуществляющим ОРД;

4) при проведении бухгалтерских и иных ревизий;

5) во время оперативно-розыскных мероприятий, проводимых правоохранительными органами (проверочная закупка, снятие информации с технических каналов связи, оперативный эксперимент, наведение справок и т.д.);

6) случайно;

7) в ходе расследования преступлений в сфере компьютерной информации;

8) при расследовании преступлений иных видов.

Несмотря на существующее разнообразие источников получения информации о преступлениях рассматриваемой категории, следует отметить, что раскрывать их не менее сложно, чем иные виды преступной деятельности. Данный факт обусловлен тем, что нередко преступники прибегают к различным уловкам, маскируют свои преступные деяния многочисленными объективными и субъективными причинами, которые действительно могут иметь место. К ним, как правило, относятся следующие:

1. *Естественные:*

· стихийные бедствия, природные явления (пожары, землетрясения, наводнения, ураганы, смерчи, тайфуны, циклоны, электромагнитные вспышки на солнце и т.п.);

· самопроизвольное разрушение элементов, составляющих СВТ.

2. *Обусловленные неумышленной деятельностью человека вследствие непреодолимых факторов:*

· ошибки при создании (изготовлении) СВТ (недочеты проектирования, в том числе системы защиты, кодирования информации, в изготовлении элементов СВТ);

· ошибки в процессе работы (эксплуатации) СВТ (неадекватность концепции обеспечения безопасности СВТ; недочеты управления системой защиты, ошибки персонала, сбои и отказы оборудования и программного обеспечения, ошибки при производстве пусконаладочных и ремонтных работ)[2];

· форс-мажорные обстоятельства, возникающие в расчетно-кредитной сфере.

Эти причины зачастую используются преступниками для сокрытия совершенных ими деяний. Во многом поэтому в большинстве случаев в процессе проведения проверок по инцидентам, возникающим в сети «Интернет», очень

сложно на первоначальном этапе определить их точную квалификацию и тем самым провести грань между должностными проступками, нарушениями в сфере гражданско-правовых отношений и преступлениями.

Анализ отечественной и зарубежной литературы, материалов конкретных уголовных дел, а также других эмпирических источников показывает, что успешное расследование преступлений рассматриваемой категории напрямую зависит от того, как быстро после их совершения начато проведение предварительного расследования.

В этой связи особую актуальность и значимость приобретает первоначальная стадия уголовного процесса – возбуждение уголовного дела. Она во многом обусловлена уголовно-правовой природой выделенных преступных посягательств, неординарностью способов их совершения, сложностью изучения исходной доказательственной информации, которая, как правило, содержится в учетных, технологических и иных документах, находящихся в сложных форматах. Помимо этого, необходимо учитывать и то обстоятельство, что все действия, составляющие данную стадию, совершаются до возбуждения уголовного дела. Поэтому эффективность работы следователя по раскрытию и расследованию преступлений в сфере предоставления услуг «Интернет» в первую очередь зависит от оперативности реагирования на заявления и сообщения о преступлении, своевременного и обоснованного принятия решения о возбуждении уголовного дела.

Практика свидетельствует о том, что запоздалое начало уголовного процесса может привести к быстрой, по сравнению с другими видами преступлений, утрате важных доказательств, безнаказанности преступников, увеличению сроков предварительного расследования и другим негативным последствиям.

Как правильно отмечал Р.С. Белкин, успешность расследования преступлений зависит не только от методически правильного подхода к процессу расследования, но и от оперативности действий, умения организовать силы и средства, которыми располагают органы, ведущие борьбу с преступностью[3].

Именно поэтому важное значение на стадии возбуждения уголовного дела о преступлениях рассматриваемой категории будет иметь оптимальная организация взаимодействия между следственными подразделениями, специализированными органами дознания, экспертными службами и специалистами, отвечающими за вопросы защиты информации, в структуре частных охранных структур (служб безопасности) в целях получения максимально полной криминалистически значимой информации о происшедшем событии.

Известно, что деятельность сотрудника органа дознания, дознавателя и следователя на начальной стадии расследования любого преступления состоит из четырех основных этапов.

1. Оценка поступившей информации о преступлении.

2. Проверка заявления и сообщения, если в исходной информации отсутствуют достаточные данные, указывающие на признаки преступления рассматриваемого вида.

3. Принятие и процессуальное оформление решения о возбуждении уголовного дела.

4. Согласование принятого решения с прокурором.

Эта деятельность регулируется уголовно-процессуальным законом и ведомственными нормативными актами, но ей присущи и определенные особенности.

Поводами и основаниями для возбуждения уголовных дел о преступлениях в сфере предоставления услуг «Интернет» чаще всего служат:

1. Заявление о преступлении, поступившее от потерпевшего – от представителя юридического лица или от гражданина (физического лица) (40 %);

2. Непосредственное обнаружение признаков преступления органом дознания (43 %):

- в результате проверки сообщения, поступившего из оперативных источников (48%), о совершенном или готовящемся преступлении;

- в ходе проведения специальных оперативно-технических мероприятий (11 %);

- по материалам контрольно-ревизионных и иных документальных проверок (28 %);

- при задержании лица (лиц) на месте совершения преступления с поличным (13 %);

3. Непосредственное обнаружение признаков преступления следователем или прокурором при расследовании уголовных дел о преступлениях других видов (9 %);

4. Сообщения в средствах массовой информации и иные поводы (8 %)[4].

В зависимости от содержания исходной информации о происшедшем событии следователь имеет возможность до возбуждения уголовного дела провести в порядке, предусмотренном ст. 144 УПК РФ, предварительную проверку фактов, изложенных в сообщении о преступлении. Естественно, такая проверка не является стадией предварительного расследования, однако она типична для преступлений в сфере предоставления услуг «Интернет». Она проводится в сроки, жестко регламентированные действующим уголовно-процессуальным законом (ч. 1 и 3 ст. 144 УПК РФ).

Поэтому целесообразно составить *план предварительной (доследственной) проверки*. В нем должны быть отражены следующие позиции:

· истребование необходимых материалов (документов), свидетельствующих о противоправности события либо отражающих незаконность проведения операций в сфере компьютерной информации и расчетно-кредитных отношений (детализация доступа в сеть «Интернет», информация об авторизации платежа, сведения о предоставленных услугах связи и т.д.);

· анализ полноты комплекта и содержания документов, подтверждающих противоправность исследуемого деяния;

· проверка подлинности и действительности документов, имеющихся в распоряжении дознавателя, органа дознания или следователя;

· получение объяснения от заявителя и возможных свидетелей (очевидцев) события:

· подготовка вопросов, подлежащих выяснению у лиц, на которых ссылается заявитель или когла имеются данные о них как о возможных свидетелях происшедшего события;

· предварительное исследование предметов и документов – возможных орудий преступления (МНИ, программ для ЭВМ, баз данных, отдельных файлов, специальных технических средств и других) В большинстве случаев до возбуждения уголовного дела исследование проводится с участием специалиста в рамках осмотра места происшествия. Заключение по результатам исследования излагается в протоколе следственного действия или приобщается к нему в письменном виде в качестве приложения (ст. 58, 80 УПК РФ). Кроме того, исследование может быть проведено специализированным органом дознания в виде оперативно-розыскного мероприятия – исследование предметов и документов (ст.6 ФЗ «Об оперативно-розыскной деятельности» № 144-ФЗ);

· ознакомление с технологией использования документированной компьютерной информации в конкретном технологическом процессе или операции;

· изучение правовой основы операции, итогом которой явилось событие, изложенное в сообщении о преступлении;

· консультации со специалистами[5];

· проведение отдельных следственных действий по закреплению следов преступления и установлению лица, его совершившего (осмотр места происшествия, освидетельствование, назначение судебной экспертизы).

В плане могут быть предусмотрены и другие проверочные и ознакомительные действия, большинство из которых не являются следственными.

С учетом данных, полученных в результате доследственной проверки поступивших материалов, принимается решение о возбуждении уголовного дела, об отказе в его возбуждении или передаче сообщения о преступлении по подследственности, определяемой ст. 151 УПК РФ.

Для принятия обоснованного решения о возбуждении уголовного дела о преступлении в сфере предоставления услуг «Интернет» в распоряжении следователя (дознавателя) должны находиться следующие сведения и документы:

1. Письменное заявление потерпевшего – гражданина или представителя юридического лица либо протокол устного заявления о преступлении в сфере услуг «Интернет».

2. Объяснение заявителя, в котором содержатся данные о времени и месте совершения преступления, предмете преступного посягательства и его индивидуальных признаках (название компьютерной информации, место ее нахождения, особые условия доступа к ней и ее МНИ и др.).

3. Документы либо их копии, подтверждающие право собственности, владения или пользования объектом, подвергшимся преступному воздействию (письменный договор на получение услуг «Интернет», электросвязи, обслуживание по банковской карте, пластиковая карта, свидетельство о праве собственности на программу для ЭВМ или базу данных и иной оформленный надлежащим образом документ).

4. Рапорт об обнаружении признаков преступления и приложенные к нему материалы, полученные в ходе производства оперативно-розыскных мероприятий, ревизий, документальных и иных проверок. При этом порядок предоставления результатов ОРД должен соответствовать требованиям, за-

крепленным в ст. 11 ФЗ «Об оперативно-розыскной деятельности» от 12.08.1995 г. и в Приказе Федеральной службы налоговой полиции РФ, ФСБ РФ, МВД РФ, Федеральной службы охраны РФ, ФПС РФ, ГТК РФ и Службы внешней разведки РФ от 13 мая 1998 г. № 175/226/336/201/286/410/56 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю, прокурору или в суд».

5. Письменное заключение специалиста о производстве предварительного исследования предметов (вещественных доказательств), а также по вопросам, поставленным перед ним лицом, производившим предварительную проверку, данное в порядке ч. 3 ст. 80 УПК РФ.

6. Идентификационные данные о владельце (собственнике, пользователе) ЭВМ, системы ЭВМ или их сети, осуществившем незаконный дистанционный доступ к охраняемой законом компьютерной информации, например: IP-адрес, логин, пароль и номер абонента сети электросвязи (номер телефона), с помощью которых был осуществлен такой доступ.

7. Протокол осмотра места происшествия – места обнаружения следов преступления с обязательным осмотром ЭВМ (сервера сети ЭВМ), МНИ и компьютерной информации, в результате которого были получены данные, подтверждающие факты, изложенные заявителем.

8. Объяснения лица, причастного к совершению противоправного деяния, в случае его установления и задержания.

Все вышеуказанные документы и содержащиеся в них сведения необходимо оценить с позиций законности, достоверности и достаточности для принятия того или иного процессуального решения.

Как показывает анализ эмпирических источников, на практике при решении вопроса о возбуждении уголовного дела допускается ряд тактических просчетов и ошибок, влияющих в конечном итоге на объективность, полноту и качество предварительного расследования. Отметим наиболее значимые из них.

Низкое качество проводимой проверки сообщения о преступлении, по материалам которой иногда необоснованно возбуждаются уголовные дела.

Очень часто материалы о преступлении в сфере предоставления услуг «Интернет», совершенном «нетрадиционным» и малопонятным по своей правовой сути (для практических работников) способом, без достаточных оснований и с нарушением всех установленных УПК сроков, оседают в органе дознания, что приводит к волоките и другим отрицательным последствиям. По этой причине лица, причастные к преступной деятельности, получают возможность скрыться от следствия, уничтожить основные следы и, таким образом, помешать установлению истины по делу.

Нередко вопреки требованиям Инструкции о порядке приема, регистрации и разрешения в органах внутренних дел Российской Федерации заявлений, сообщений и иной информации о происшествиях, утвержденной Приказом МВД России от 01.12.2005 г. № 985, заявления о преступлениях рассматриваемой категории регистрируются с большим опозданием, а иногда и вовсе не регистрируются.

Чтобы не допускать рассмотренные просчеты, следует всегда помнить, что успех расследования преступления в сфере предоставления услуг «Интернет» обеспечивают быстрота и решительность действий следователя в самые первые часы производства по делу, организованное взаимодействие со специализированным органом дознания – отделом «К» Управления специальных технических мероприятий (УСТМ) УВД (ГУВД, МВД) области (края, республики), а также наличие соответствующего специалиста[6].

Например, в отдельных случаях оперативные работники должны выяснить (проверить) некоторые конкретные вопросы и материалы, произвести задержание преступника, выполнить другие мероприятия оперативного характера. Промедление при этом недопустимо, так как может привести к утечке конфиденциальной информации, утрате материальных следов, уничтожению документов и идентификационных признаков предметов, которые в дальнейшем могут использоваться в качестве вещественных доказательств.

Помимо вышеуказанного, *на момент принятия решения о возбуждении уголовного дела следователь должен:*

а) иметь четкое и полное представление о характере деятельности и структуре объекта, где было совершено преступление;

б) знать конкретные условия деятельности объекта, связанные с предметом преступного посягательства, существующий порядок учета и отчетности, систему оборота товаров и документов на машинных носителях;

в) располагать коммуникативными и иными тактико-техническими характеристиками используемой компьютерной техники;

г) знать организацию охраны конфиденциальной компьютерной информации;

д) разбираться в служебных обязанностях лиц, имеющих прямые или косвенные отношения к предмету преступления[7].

Для того чтобы детально разобраться в особенностях деятельности потерпевшего, следователю необходимо ознакомиться с соответствующей справочной литературой, изучить ведомственные нормативные акты. Исключительно важное значение при расследовании преступлений выделенной группы имеют консультации со специалистами, в качестве которых могут выступать любые лица, обладающие необходимыми знаниями и опытом. Ими могут быть квалифицированные работники различных организаций, осуществляющие свою деятельность в области компьютерных и телекоммуникационных технологий, а также профессионально занимающиеся защитой информации, охраняемой законом. Предпочтение следует отдавать сотрудникам Федеральной службы по техническому и экспортному контролю, действующей на основании Указа Президента Российской Феде-рации № 1085 от 16.08.2004 г. «Вопросы Федеральной службы по техническому и экспортному контролю»; специалистам, производящим судебные компьютерно-технические экспертизы; сотрудникам служб безопасности, которые занимаются вопросами защиты информации от ее утечки по техническим каналам; работникам научно-исследовательских центров (институтов, лабораторий) и учебных заведений.

Примечания

[1] Данные ГИЦ МВД РФ.

[2] Вехов, В.Б. Тактические особенности расследования преступлений в сфере компьютерной информации: науч.-практ. пособие. 2-е изд., доп. и испр. / В.Б.Вехов, В.В.Попова, Д.А.Илюшин. – М.: ЛексЭст, 2004. – С. 40.

[3] Белкин, Р.С. Курс криминалистики: в 3 т. Т. 1 // Общая теория криминалистики/ Р.С.Белкин. – М., 1997. – С. 307.

[4] Данные, полученные в ходе изучения материалов уголовных дел, возбужденных и расследованных следственными подразделениями ОВД восьми субъектов РФ.

[5] Вехов, В.Б. Указ. соч. – С.42

[6] Там же. – С. 46.

[7] См.: Вехов, В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники: учеб. - метод. пособие. 2-е изд., доп. и испр. /В.Б. Вехов. – М., 2000. – С. 18-19.

Статья принята в печать в окончательном варианте 13.12.2006 г.

D.A. Ilyushin

PECULIARITIES STARTING CRIMINAL CASES, OF ADMITTED IN THE SPHERE OF INTERNET SERVICES

In the article author reveals in detail main reasons and motives for bringing such kind of lawsuits, offers the concrete scheme of interaction between the investigator and other colleagues of inquiry department. There are also touched upon some points having a practical matter for improvement of inquiry work of law guard government.