Е.А. Жегалов

Тактическая операция по собиранию информации о преступлении, связанном с использованием электронной почты

В последнее десятилетие в России активно внедряются в хозяйственную деятельность, науку и быт компьютерные технологии. Это не могло не сказаться на способах преступной деятельности, которую в этой сфере достаточно трудно обнаружить. По независимым данным, уровень латентности преступлений в сфере компьютерной информации на Западе – 70–80%, а в России – 90–93% [1]. Представляется важным изучение не только данных преступлений, но и любых других, способ подготовки и совершения которых связан с использованием компьютеров и глобальной компьютерной системы Интернет. В этой связи очевиден ряд вопросов. При каких условиях фактические данные, полученные из виртуальной компьютерной системы, могут являться доказательствами по уголовному делу? Как, посредством каких технических средств, процессуальных действий и тактических приемов можно их добыть? Первые научные работы на эту тему не могут, естественно, охватить все без исключения проблемы [2].

При расследовании преступлений в сфере внешнеэкономической деятельности чрезвычайно актуальны особенности тактики следственных действий, подготовка, совершение, сокрытие которых происходило посредством компьютерной системы Интернет и, в частности, с помощью электронной почты. Информационное взаимодействие во внешнеэкономической деятельности не может не осуществляться все более и более современными способами. Система Интернет превратилась в огромное виртуальное поле социальной деятельности, посредством которого происходит обмен информацией от заключения сделок до простого общения. Невинная компьютерная переписка о дате прилета, месте встречи на самом деле может оказаться согласованием способа, места и времени приготовления, сокрытия или совершения преступления.

Государство оказалось не готово к пресечению преступной деятельности в этой сфере. Объем, порядок и сроки хранения как самой электронной переписки, так и информации о ней (адреса отправителя и получателя, время отправления и получения корреспонденции и т.д.), определяются в настоящее время не правовыми нормами, а техническими возможностями того или иного провайдера (организации, предоставляющей пользователю электронный адрес). Проблема использования компьютерной информации из электронной почты в качестве доказательства осложняется еще и тем, что по своей сути эта информация является почтово-телеграфным сообщением, а ограничение права на тайну таких сообщений допускается только на основании судебного решения (ст. 23 Конституции Российской Федерации).

Б., имея умысел уклониться от уплаты таможенных платежей при покупке дорогого автомобиля, направляла через Интернет письма с электронного адреса из России в Англию. В письмах она предлагала Д. выступить подставным лицом в качестве покупателя автомобиля с целью получения на ее имя льгот по таможенным платежам как на лицо, находящееся за границей более шести месяцев. В данных сообщениях согласовывались время и место встречи с представителем фактического покупателя, устанавливалось вознаграждение за такую услугу, определялся круг обязанностей. Посредством ответа по электронной почте было получено согласие. В результате совершено уклонение от уплаты таможенных платежей на сумму 100130 руб. После прибытия в Россию был применен еще один (другой) способ сокрытия преступления. Содержание переписки явилось важным доказательством прямого умысла виновных (см.: Архив Новосибирской таможни за 1999 год. Наблюдательное производство по уголовному делу №404).

Такие преступления возможны не только в таможенной, но и в кредитно-банковской, научной, любой другой сфере деятельности. Часто доказательство самого факта переписки имеет огромное значение для расследования. Как показывает опыт, решение тактической задачи расследования по получению допустимыми способами наиболее полных фактических данных о наличии и содержании переписки между определенными субъектами по каналам в Интернете не может быть достигнуто одним следственным действием. Учение о тактической операции, как о комплексе мер и действий при решении задач расследования, предложенное А.В. Дуловым [3], развитое В.И. Шикановым [4], служит основой для правильного построения тактики собирания компьютерной информации о наличии и содержании электронной переписки. Такая тактическая операция может быть нескольких типов в зависимости от того, осуществлялась оперативно розыскная деятельность до возбуждения уголовного дела или нет.

Основное содержание операции второго типа следующее. При получении информации о факте переписки по электронной почте следователь

(орган дознания) на первом этапе принимает меры к установлению личностей, адресов и телефонов абонентов, а также электронного адреса «почтового ящика» в России. Желательно процессуальным путем (в ходе выемки, обыска, осмотра и т.д.) получить дискету с отправленной или полученной информацией искомого пользователя. Затем, посредством опроса специалистов, определяется место офиса организации (провайдера), предоставившей электронный адрес. Например, электронный адрес «NEO@SINET.RU» означает, что пользователь электронной почты (@), имеет имя (NEO), которое ему предоставила организация, находящаяся в России (RU), имеющая электронное название (SIBNET). Успех дальнейших действий определяет умелое использование фактора внезапности, без учета которого тактическая задача данного этапа вряд ли будет решена [5, с. 244–275]. В случае если пользователь узнает, что им интересуется следствие, он может очень быстро уничтожить информацию путем входа в электронную сеть под своим паролем с места любого другого пользователя. Уничтожить информацию можно через знакомых, попросив их об этом по текстовому пейджеру или телефону. В свою очередь, если следователю удастся внезапно одновременно изъять все имеющиеся носители информации и документы об оказании услуг электронной почты конкретному лицу, то сразу после этого посредством прослушивания телефонных переговоров можно получить данные еще и о связях и отношениях пользователя с соучастниками, если тот, застигнутый врасплох, будет давать сообщникам указания по телефону или вести переговоры по поводу изъятой информации.

Вторым этапом операции является установление места нахождения компьютеров пользователя и получение решения суда об ограничении права лица на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений в целях расследования конкретного уголовного дела. Порядок получения таких решений установлен постановлением Пленума Верховного Суда Российской Федерации от 24 декабря 1993 г. №13 [6]. Данное решение суда и ордер на обыск в жилище и на рабочем месте субъекта обеспечивает законность дальнейшего получения информации и ее допустимость в качестве доказательства. Целесообразно на основании этого же решения приступить к прослушиванию телефонных переговоров. После этого в офисе организации (провайдера) производятся выемка договора на оказание услуг электронной связи и допрос сотрудников. Все участники следственных действий предупреждаются о недопустимости разглашения данных предварительного следствия (ст. 139 УПК РСФСР). В случае если удастся получить оригинал договора, из него будет известна вторая часть электронного адреса – личный пароль пользователя, знание которого в дальнейшем облегчит осмотр и экспертизу системных блоков компьютеров. Если у провайдера не сохранились тексты самих сообщений, необходимо принять меры к изъятию информации из электронного журнала корреспонденции о дате, времени, адресах лиц, осуществлявших электронную переписку. Обычно информация в электронном журнале хранится не более шести месяцев. Сразу после выемки у провайдера организуется одновременный обыск во всех местах нахождения компьютеров пользователя, особое внимание обращается на внезапность и одновременность проникновения в помещения. Рекомендуется привлекать к производству обыска специалиста. В протоколе, кроме прочего, необходимо отразить сведения о том, исправен ли компьютер, сколько информации содержал системный блок до изъятия (в байтах), какими операционными системами и программами он был оснащен. Необходимо обнаружить и изъять все другие носители информации (дискеты и т.п.). Целесообразно немедленно допросить в качестве свидетелей всех лиц, находящихся в местах производства обысков.

Завершающим этапом данной тактической операции является компьютерно-техническая (информационно-техническая) экспертиза. Перед экспертом, кроме общеизвестных [7, с. 961–963], могут быть поставлены следующие вопросы.

1. Какая информация содержится на дискетах, полученных в ходе осмотра и обыска (выемки), каково назначение этой информации, происхождение, содержание?

2. Какая информация на указанных дискетах передавалась по электронной почте, в какое время, каковы электронные имена отправителя и получателя?

3. Информация на предоставленных дискетах образовалась после передачи по электронной почте или механически напечатана?

4. Имеется ли в системных блоках компьютеров и дискетах, полученных в ходе обысков тогда-то, информация, идентичная той, которая находится на дискетах, полученных тогда-то в ходе осмотра?

5. Существует ли конструктивная возможность передавать информацию по электронной почте с представленных системных блоков компьютеров, если да, то каковы электронные адреса отправителей и получателей почты?

6. Передавалась ли информация, хранящаяся на дискетах, полученных тогда-то в ходе осмотра, через системные блоки изъятых компьютеров по электронной почте, если да, то с какого именно компьютера, какое именно сообщение?

7. Содержится ли в системных блоках этих компьютеров информация, отправленная и полученная по электронной почте абонентами с электронными именами такими-то, каковы ее содержание, время создания, отправления, получения?

Фрагменты текстов из заключения экспертов на иностранном языке переводятся по правилам уголовно-процессуального закона.

Криминалистические аспекты работы с компьютерной информацией требуют дальнейшего творческого развития на основе учения о тактических операциях. Необходимо законодательно урегулировать вопрос о контроле над глобальными информационными системами, действующими на территории России. Нужно установить объем и место хранения информации о прошедших сообщениях, сроки хранения самих сообщений, перечень документов о присвоении и изменении электронных адресов физическим и юридическим лицам, порядок работы коллективных пользователей с целью возможности установления личности автора сообщения.

Литература

1. Пичугин И. Управление «Р» показало когти // Коммерсантъ. 1999. 13 авг.

2. См.: Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений: Автореф. … дис. канд. юрид. наук. М., 1997.

3. Дулов А.В. Тактические операции при расследовании преступлений. Минск, 1979.

4. Шиканов П.И. Теоретические основы тактических операций в расследовании преступлений. Иркутск, 1983.

5. Белкин Р.С. Курс криминалистики: В 3-х т. Т. 3: Криминалистические средства, приемы и рекомендации. М., 1997.

6. Бюллетень Верховного Суда Российской Федерации. 1994. №3.

7. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика. М., 1999.