

К ВОПРОСУ ОБ ОСОБЕННОСТЯХ ОСМОТРА МЕСТА ПРОИСШЕСТВИЯ ПО ДЕЛАМ О КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЯХ

Т. П. Ишмаева

Южно-Уральский государственный университет (национальный исследовательский университет), г. Челябинск, Российская Федерация

В статье рассматриваются вопросы об особенностях закрепления в отечественном уголовном законодательстве ответственности за действия, совершенные в области компьютерных технологий; тактические особенности осмотра места происшествия по делам о компьютерных преступлениях.

Ключевые слова: компьютерные технологии, уголовная ответственность, осмотр места происшествия, специалист, компьютерные преступления.

TO THE PECULIARITIES OF CRIME SCENE EXAMINATION IN CASES ON CYBERCRIMES

T. Ishmaeva

South Ural State University (National Research University), Cheliabinsk, Russian Federation

The article deals with the peculiarities of introducing the responsibility for acts committed in the field of computer technology in domestic Criminal Law, as well as with tactical peculiarities of crime scene examination in cases on cybercrimes.

Keywords: computer technology, criminal responsibility, crime scene examination, specialist, cybercrimes.

Стремительность развития информационных отношений, информационно-коммуникационных технологий, киберпространства, компьютерных социальных сетей, тотальная компьютеризация общества, появление новых технических средств создания, использования, обработки и распространения цифровой информации в современном мире поражает. И в таких динамичных условиях нашего времени общество постоянно сталкивается с проблемами различного характера, порождение которых зачастую вызвано стремлением к созданию более совершенных и эффективных моделей существования. Это в полной мере относится и к такой специфической сфере, как область применения электронной техники и информационных технологий, которая все более быстрыми темпами внедряется в современную жизнь мирового сообщества. Безусловно, являясь в современных условиях неотъемлемой сферой общественной жизни, данная отрасль привлекает очень активное внимание со стороны преступного элемента.

Между тем большинство населения, используя компьютер в личных или служебных целях, имеет слабое представление о программировании и программном обеспечении, средствах антивирусной защиты и их возможностях. В связи с этим все более актуальным становится вопрос о защите компьютерной информации граждан, муниципальных и государственных учреждений, предприятий, органов власти от несанкционированного доступа к компьютерной информации, вредоносных компьютерных программ. Проблема криминализации деяний, связанных с компьютерной информацией, обусловлена ростом компьютерных преступлений и сомнений не вызывает. Так, в 2014 году по данным МВД России¹, было зарегистрировано порядка 11 000 киберпреступлений.

Отечественное законодательство устанавливает в Уголовном кодексе РФ ответственность за действия, совершенные в области компьютерных технологий. Все виды указанных деяний объединены в главе 28

¹ <https://mvd.ru>

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ В ОВД

«Преступления в сфере компьютерной информации». Однако понятие «компьютерное преступление» закреплено не было. В связи с этим, используя международные подходы, можно вести речь о наличии такой категории преступлений в национальной практике. Исходя из того, что видовым объектом указанной группы преступлений является информационная безопасность, а предметом – компьютерная информация, то под компьютерными преступлениями, думается, целесообразно понимать совершенные виновно общественно опасные деяния, направленные против охраняемых уголовным законом общественных отношений в сфере информационных процессов (информационная безопасность компьютерных сетей и систем).

Создание вредоносной компьютерной программы или иной компьютерной информации означает любую сознательно-волевую деятельность лица, направленную на разработку совокупности электронно-цифровых данных и команд, предназначенных для функционирования в компьютерах, информационно-телекоммуникационных сетях или иных устройствах хранения, обработка и передачи компьютерной информации, в том числе путем внесения изменений в уже существующие вредоносные программы с целью их совершенствования, для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Создание вредоносной программы следует считать оконченным с момента, когда она приобрела вредоносные свойства и готова к использованию. Распространение вредоносной компьютерной программы или иной компьютерной информации означает ее передачу (копирование) другим лицам любым путем, включая продажу, дарение, обмен, прокат, сдачу внаем, предоставление взаймы (например, размещение на хакерских сайтах, в сети Интернет, по электронной почте и т. д.).

Интересно, что в этом случае снова образуется некоторая проблема – законодатель не дает определения понятия «вредоносная компьютерная программа», однако указывает на то, что это компьютерная программа либо компьютерная информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств

защиты компьютерной информации. Информацию со встроенными в нее вредоносными программными кодами можно отнести к иной компьютерной информации, предназначеннной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты [3, с. 156]. Таким образом, представляется возможным сделать вывод, что вредоносные компьютерные программы – это специальные компьютерные программы, созданные с целью несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, а также совершения иных противоправных деяний (например, рассылка спама, фишинга, кибершпионажа, кибершантажа, управление зараженным компьютером, создание ботнетов и др.).

Думается, что наиболее опасной разновидностью вредоносной программы, является вирусная программа. Вирусная программа обладает способностью дистанционного заражения компьютеров, самокопирования и самораспространения через информационную сеть Интернет, социальные информационные сети, электронную почту, Wi-Fi, Bluetooth, sms- и mms-сообщения.

Определенную сложность вызывает не только детальная уголовно-правовая (терминологическая) характеристика, а также и расследование данной категории дел. Практическим работникам правоохранительных органов довольно сложно расследовать данную категорию дел по ряду объективных и субъективных причин. Так, например, сотрудникам, осуществляющим работу по своевременному раскрытию и дальнейшему расследованию выявленных преступлений, необходимо владеть знаниями компьютерных и информационных технологий. В частности, при производстве следственных действий, связанных с изъятием вещественных доказательств.

Первоначальным и неотложным следственным действием по делам о киберпреступлениях, как и по делам об иных видах преступлений, является осмотр места происшествия. И уже на данном первоначальном этапе, необходимо учитывать ряд тактических особенностей, присущих лишь данной категории дел. Следует уточнить в контексте рассматриваемой темы, что осмотр – это непосредственное обнаружение, восприятие и исследование следователем материальных

объектов, имеющих отношение к исследуемому событию [6, с. 458].

Основными целями проведения осмотра места происшествия по делам о компьютерных преступлениях являются:

установление обстоятельств, произошедшего события (способ, место, время совершения преступления, личность совершившего преступное посягательство и пр.) путем исследования обнаруженных признаков преступления;

выявление, фиксация, изъятие и оценка следов преступления (как традиционных криминалистических, так и нетрадиционных – информационных следов преступлений в сфере компьютерной информации), различных вещественных доказательств;

получение информации, необходимой для построения и проверки следственных версий и осуществления розыскной работы по делу [8, с. 200].

В контексте рассматриваемого вопроса актуальной является проблема определения места происшествия. При совершении одного преступления, например неправомерного доступа к компьютерной информации, может быть несколько мест происшествия:

рабочее место, рабочая станция – место обработки информации, ставшей предметом преступного посягательства;

место постоянного хранения или резервирования информации – сервер или стример;

место использования технических средств для неправомерного доступа к компьютерной информации, находящейся в другом месте, при этом место использования может совпадать с рабочим местом, но находится вне организации, например при стороннем взломе путем внешнего удаленного сетевого доступа;

место подготовки преступления (разработки вирусов, программ взлома, подбора паролей) или место непосредственного использования информации (копирование, распространение, искажение).

Местом происшествия может быть одно помещение, где установлен компьютер и хранится информация, ряд помещений, в том числе в разных зданиях, расположенных на различных территориях, либо участок местности, с которого проводится дистанционный электромагнитный или аудиоперехват.

На современном этапе выделяется новое для современной практики место совершения преступления, а именно информационное пространство (киберпространство), где

не действуют географические, юридические законы и понятия. И вполне справедливо выделяется ряд вопросов о специфических особенностях при проведении осмотра места происшествия. Ввиду специфики компьютерных преступлений для обнаружения следов преступлений в процессе осмотра места происшествия необходимо наличие специальных знаний в области компьютерных технологий [7, с. 72].

Лица, занимающиеся расследованием данного рода преступлений, и работники судебной системы в большинстве своем не обладают специальными познаниями в области новых компьютерных технологий, что влечет ошибки в расследовании [5, с. 28]. Применительно к киберпреступлениям важно обратить внимание на то, что для успешного выявления, быстрого и полного расследования этих преступлений необходимы новые подходы, основанные на более полном использовании достижений науки и техники, при содействии сведущих лиц.

Целесообразно по делам о киберпреступлениях привлекать к осмотру места происшествия специалистов из числа:

сотрудников экспертных подразделений всех уровней и различной ведомственной принадлежности;

представителей научных и педагогических коллективов, обладающих глубокими познаниями в области информационных технологий;

частных лиц, не состоящих в штате каких-либо официальных структур [2, с. 182].

В то же время, привлекая специалиста к участию в осмотре места происшествия, следователю важно убедиться в его компетентности. На практике совершается огромное количество ошибок из-за привлечения некомпетентного специалиста, не владеющего необходимыми знаниями. Например, возникали случаи, когда привлекали квалифицированного пользователя ПК, но не владевшего навыками обращения с большими вычислительными комплексами, что вызывало проблемы при проведении следственного действия. В связи с этим важно привлекать специалистов с необходимым профилем знаний, в зависимости от целей и задач осмотра, с учетом первоначальных данных о характере преступления [1, с. 12].

Еще одной из самых часто совершаемых на практике ошибок следователя является неправильная упаковка и транспортировка компьютерно-технических средств при изъятии их в ходе осмотра места происшествия.

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ В ОВД

Исследователи предлагают ряд рекомендаций, поддерживаемых практическими работниками [4, с. 104]:

изымается компьютерная техника только в выключенном состоянии;

при отсоединении устройств в протоколе и в схемах обязательно указывается и отображается порядок соединения, при необходимости все разъемы и кабели маркируются;

очень важно при наличии канала связи установить и зафиксировать тип связи, а также абонентский номер, используемую аппаратуру и рабочую частоту;

системные блоки при изъятии обязательно опечатываются для исключения возможности разукомплектования, физического повреждения, изменения, удаления содержащейся в них информации в отсутствие владельца или эксперта, следователя. Системный блок опечатывается листом бумаги с подписями следователя, собственника и понятых, который прикрепляется на лицевую и заднюю панель компьютера и захлестываеться на боковые стенки. Конечно, существуют и другие способы опечатывания, следователь выбирает их в зависимости от устройства корпуса системного блока. Главное, чтобы была исключена возможность подключения или разборки системного блока, без повреждения опечатки;

необходимо соблюдать особые условия хранения и перемещения системных блоков, исключающие повреждение информации на носителях, например, вред могут нанести электромагнитные излучения и поля, поэтому для предотвращения вреда металлоискатели, сильные осветительные приборы и другие мощные источники магнитного поля к компьютерной технике нельзя подносить ближе, чем на 1 м.

транспортировка изъятого оборудования должна осуществляться с учетом всех вышеперечисленных требований, при этом важно исключить механическое воздействие на оборудование, влияние электромагнитных лучей и полей, атмосферных факторов, а также высоких и низких температур, влекущих повреждение аппаратуры.

Еще одну особенность необходимо учитывать при производстве осмотра места происшествия – если компьютер работает,

ситуация для следователя, существенно осложняется, однако и в этом случае не следует отказываться от изъятия необходимых данных. Самое правильное решение здесь – привлечение специалиста при изъятии объектов. Однако можно выделить ряд рекомендаций и в такой ситуации:

а) определить, какая программа выполняется. Для этого необходимо изучить изображение на экране дисплея и по возможности детально описать его. Можно осуществить фотографирование или видеозапись изображения;

б) остановить исполнение программы. Остановку можно осуществить также с использованием «Диспетчера файлов», либо одновременным нажатием клавиш Ctrl-C или Ctrl-Break;

в) зафиксировать (отразить в протоколе) результаты своих действий и реакции компьютера на них;

г) определить наличие у компьютера внешних устройств, накопителей информации на жестких магнитных дисках и картах памяти, виртуального диска;

д) определить наличие у компьютера внешних устройств удаленного доступа к системе и определить их состояние (отразить в протоколе), после чего разъединить сетевые кабели так, чтобы никто не мог изменить или уничтожить информацию в ходе обыска (например, отключить телефонный шнур из модема);

е) скопировать программы и файлы данных. Копирование осуществляется стандартными средствами операционной системы;

ж) выключить подачу энергии в компьютер.

Осмотр места происшествия – первоначальное неотложное следственное действие, промедление в проведении которого может повлечь утрату доказательственной информации. Учитывая специфику компьютерных преступлений, расследование данной категории дел представляет собой определенную сложность. Особой специфики требует проведение осмотра места происшествия – для обнаружения следов преступлений в процессе осмотра места происшествия по делам о киберпреступлениях необходимо наличие специальных знаний в области компьютерных технологий.

Примечания

- Гаврилов М. Осмотр места происшествия при расследовании преступлений в сфере компьютерной информации // Законность. – 2011. – № 9. – С. 11-16.
- Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. – М., 2012. – С. 182.

3. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. Г. А. Есакова. – М., 2014. 4. Менжега М. М. Методика расследования создания и использования вредоносных программ для ЭВМ. – М., 2013.
5. Протасевич А. А. Борьба с киберпреступностью как актуальная задача современной науки. – М., 2011. – С. 28-33.
6. Россинская Е. Р. Судебная экспертиза в гражданском, административном и уголовном процессе. – М., 2012.
7. Хомков В. П. Организационно-правовые аспекты расследования и предупреждения преступлений в сфере компьютерной информации: дис. ... канд. юрид. наук. – Иркутск, 2004.
8. Шурухнов Н. Г. Расследование неправомерного доступа к компьютерной информации. – М., 2014.

ИШМАЕВА Татьяна Павловна,
старший преподаватель кафедры уголовно-правовых дисциплин факультета
Подготовки сотрудников правоохранительных органов, Южно-Уральский
государственный университет (национальный исследовательский университет).

E-mail: ishmaev.at@mail.ru

ISHMAEVA Tatyana, senior lecturer, Chair of Criminal-and-Legal Subjects,
Faculty of Law Enforcement Officers' Training, South Ural State University (National Research
University).

E-mail: ishmaev.at@mail.ru