УДК 343.985.4
ББК 67.522.1

А. А. Протасевич
доктор юридических наук, профессор,
Байкальский государственный университет
экономики и права

Л. П. Зверянская
Байкальский государственный университет
экономики и права

ОСОБЕННОСТИ ОСМОТРА МЕСТА ПРОИСШЕСТВИЯ ПО ДЕЛАМ О КИБЕРПРЕСТУПЛЕНИЯХ

Авторы исследуют проблемные вопросы осмотра места происшествия по делам о киберпреступлениях. Анализируются вопросы «специфического» осмотра места происшествия, вопросы привлечения специалистов в сфере информационных технологий, типичные ошибки следователей при проведении осмотра места происшествия.

Ключевые слова: киберпреступления; компьютерные преступления; осмотр места происшествия.

A. A. Protasevich
Doctor habil. (Law), Professor,
Baikal State University of Economics and Law

L. P. Zveryanskaya
Baikal State University of Economics and Law

PECULIARITIES OF CYBERCRIME SCENE INVESTIGATION

The authors explore problems of cybercrime scene investigation (CSI), analyze the issues of «specific» CSI involving IT-specialists, and investigators' typical errors.

Keywords: cybercrimes; computer crimes; crime scene investigation (CSI).

Основным источником объективной информации о преступлении является такое типичное следственное действие, как осмотр места происшествия. При проведении осмотра следователь имеет возможность сбора информации о наличии признаков преступления, его механизме и обстоятельствах совершения, а также возможность фиксации обнаруженного.

Основные цели проведения осмотра места происшествия по делам о компьютерных преступлениях:

– 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 [6, с. 200].

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2013. № 2
http://eizvestia.isea.ru

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2013. № 2
http://eizvestia.isea.ru

В настоящее время существует 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 находиться 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), полученной в результате неправомерного доступа к данным, содержащимся на ПК.

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.

Также современные ученые выделяют новое для современной практики место совершения преступления, а именно информационное пространство (киберпространство), где не действуют географические, юридические законы и понятия. Существует ряд вопросов, как проводить специфический осмотр места происшествия, как фиксировать найденную информацию и придавать ей доказательственное значение.

Поэтому ввиду специфики компьютерных преступлений для обнаружения следов преступлений в процессе осмотра места происшествия необходимо наличие специальных знаний в области компьютерных технологий [7, с. 72–73]. «Специальные познания, это познания, основанные на системе теоретических знаний в соответствующей области и приобретенные субъектом в процессе практической деятельности путем специальной подготовки или профессионального опыта» [1, с. 398].

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]. Данное утверждение подтверждают результаты опроса правоохранительных, правоприменительных органов и специалистов в области IT-сферы: только 40 % следователей владеют компьютером на уровне обычного пользователя, 40 % не разбираются и не понимают процесс работы компьютера. Так же интересен факт того, что 95 % из числа опрошенных программистов считают, что на сегодняшний день без участия профессионала найти нужную, «скрытую» информацию в компьютере без риска ее уничтожения довольно сложно.

Применительно к киберпреступлениям исследователи замечают, 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.

Привлечение к участию в следственных действиях специалистов или экспертов в области информационных технологий способствует рассле-

дованию киберпреступлений, затрудняя сообщение ложных данных, скрытие важной для расследования информации, а также оказывая техническую помощь следствию, предохраняя его от совершения ненужных действий, направленных на уничтожение важных доказательств.

Анализ криминалистической, специальной литературы и следственной практики показал, что помощь специалиста следователю в работе со следами на месте происшествия может заключаться:

– в обнаружении, фиксации и изъятии следов с помощью средств криминалистической техники;

– в описании следов в протоколе, составлению планов и схем их расположения;

– в консультациях по вопросам изучения следов;

– в отборе следов криминалистического исследования.

По делам о киберпреступлениях специалисты могут привлекаться 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 [3, с. 182].

В тоже 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 [2, с. 11].

Как показала следственная практика, лучше всего привлекать к осмотру места происшествия экспертов, которые в дальнейшем будут проводить компьютерно-техническую экспертизу.

Также для участия в осмотре места происшествия в качестве понятых необходимо привлекать людей, разбирающихся в процессах работы компьютерной техники, чтобы исключить возможные негативные последствия в виде заявлений заинтересованных лиц об изменении и удалении следователем информации, содержащейся в ПК или иной компьютерной технике.

Одними из самых часто совершаемых на практике ошибок следователя являются неправильная упаковка и транспортировка компьютерно-технических средств при изъятии их в ходе осмотра места происшествия. Вследствие этого необходимо отметить следующие моменты:

– 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;

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2013. № 2
http://eizvestia.isea.ru

– системных блоков 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 захлестывается 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 [4, с. 103–104].

Список использованной литературы

1. Белкин Р. С. Криминалистика : учеб. пособие / Р. С. Белкин. — М. : НОРМА : ИНФРА-М, 2000. — 990 с.

2. Гаврилов М. Осмотр места происшествия при расследовании преступлений в сфере компьютерной информации / М. Гаврилов, А. Иванов // Законность. — 2001. — № 9. — С. 11–16.

3. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью / В. Е. Козлов. — М. : Горячая линия-Телеком, 2002. —336 с.

4. Менжега М. М. Методика расследования создания и использования вредоносных программ для ЭВМ / М. М. Менжега. — М. : Юрлитинформ, 2010. — 165 с.

5. Протасевич А. А. Борьба с киберпреступностью как актуальная задача современной науки / А. А. Протасевич, Л. П. Зверянская // Криминологический журнал Байкальского государственного университета экономики и права. — 2011. — № 3. — С. 28–33.

6. Расследование неправомерного доступа к компьютерной информации : учеб. пособие / под ред. Н. Г. Шурухнов. — 2-е изд. — М. : Моск. ун-т МВД России, 2004. — 352 с.

7. Хомколов В. П. Организационно-правовые аспекты расследования и предупреждения преступлений в сфере компьютерной информации : дис. … канд. юрид. наук : 12.00.09 / В. П. Хомколов. — Иркутск, 2004. — 200 с.

References

1. Belkin R. S. *Kriminalistika* [Criminalistics]. Moscow, NORMA Publ., INFRA-M Publ., 2000. 990 p.

2. Gavrilov M., Ivanov A. Crime scene investigation in computer crimes inquiry. *Zakonnost – Legalness*, 2001, no. 9, pp. 11–16 (in Russian).

3. Kozlov V. E. *Teoriya i praktika borby s kompyuternoy prestupnostyu* [Theory and practices of fighting computer crimes]. Moscow, Goryachaya liniya-Telekom Publ., 2002. 336 p.

4. Menzhega M. M. *Metodika rassledovaniya sozdaniya i ispol'zovaniya vredonosnykh programm dlya EVM* [Techniques of investigating creation and use of malware]. Moscow, Yurlitinform Publ., 2010. 165 p.

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2013. № 2
http://eizvestia.isea.ru

5. Protasyevich A. A., Zveryanskaya L. P. Fighting cybercrimes as an urgent task for contemporary research. *Kriminologicheskiy zhurnal Baykalskogo gosudarstvennogo universiteta ekonomiki i prava – Criminology Journal of Baikal National University of Economics and Law*, 2011, no. 3, pp. 28–33 (in Russian).

6. Gavrilin Yu. V., Pushkin A. V., Sotskov E. A., Shurukhnov N. G. *Rassledovanie nepravomernogo dostupa k kompyuternoy informatsii* [Investigation of unauthorized access to computer information]. Moscow, Moskovskiy universitet MVD Rossii Publ., 2004. 352 p.

7. Khomkolov V. P. *Organizatsionno-pravovye aspekty rassledovaniya i preduprezhdeniya prestupleniy v sfere kompyuternoy informatsii. Kand. dis.* [Organizational and legal aspects of investigation and prevention of cybercrimes. Cand. Dis.]. Irkutsk, 2004. 200 p.

Информация об авторах

Протасевич Александр Алексеевич — доктор юридических наук, профессор, декан судебно-следственного факультета, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, 11, e-mail: kupik@isea.ru.

Зверянская Лариса Павловна — аспирант, кафедра уголовного процесса и криминалистики, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, 11, e-mail: zveryanskayaL@mail.ru.

Authors

Protasevich Aleksandr Alekseevich — Doctor habil. (Law), Professor, Dean, Faculty of Judicial Enquiry, Baikal State University of Economics and Law, 11 Lenin st., 664003, Irkutsk, Russia, e-mail: kupik@isea.ru.

Zveryanskaya Larisa Pavlovna — PhD student, Dep-t of Criminal Procedure and Criminalistics, Baikal State University of Economics and Law, 11 Lenin st., 664003, Irkutsk, Russia, e-mail: zveryanskayaL@mail.ru.

http://eizvestia.isea.ru
2013. № 2
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ