2. Бескова И. А. Феномен сознания : монография / И. А. Бескова, И. А. Герасимова, И. П. Меркулов. – М. : Прогресс-Традиция, 2010. – 366 с.
3. Вишневецкий К. В. Особенности криминалистической фото- и видеофиксации материальных и идеальных следов взрыва / К. В. Вишневецкий // Общество и право. – 2011. – № 2. – С. 23–25.
4. Сборник документов по истории государства и права зарубежных стран. – Иркутск : ИГУ, 1973. – Вып. 1. – 81 с.
5. Соколова О. А. Актуальные направления комплексного подхода к изучению личности человека в предупреждении, раскрытии и расследовании преступлений / О. А. Соколова // Эксперт-криминалист. – 2013. –№ 3. – С. 9–11.
6. Спасович В. Д. О теории судебно-уголовных доказательств / В. Д. Спасович. – Петербург : Тип. Правительствующего Сената, 1864. – 112 с.
7. Суворова Л. А. Идеальные следы в криминалистике : автореф. дис. … канд. юрид. наук / Л. А. Суворова. – Воронеж, 2005. – 24 с.
8. Фельдштейн Г. С. Лекции по уголовному процессу / Г. С. Фельдштейн. – М. : Тип. В. Рихтер, 1915. – 432 с.

Информация об авторе

Славгородская Ольга Александровна – кандидат юридических наук, доцент кафедры криминалистического обеспечения расследования преступлений, ФГБОУ ВПО «Саратовская государственная юридическая академия», Саратов (Россия), e-mail: slavkur-htc@yandex.ru.

Information about the author

Slavgorodskaya Olga Aleksandrovna – Ph.D., assistant professor of forensic crime investigation software, VPO «Saratov State Law Academy», Saratov (Russia), e-mail: slavkur-htc@yandex.ru.

УДК 343.985
ББК 67.523

И.Г. Смирнова
О.А. Егерева

НЕКОТОРЫЕ ПРОБЛЕМЫ, ВОЗНИКАЮЩИЕ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И КОМПЬЮТЕРНЫХ СЕТЯХ: К ВОПРОСУ О КРИМИНАЛИСТИЧЕСКОМ АСПЕКТЕ СОБИРАНИЯ ДОКАЗАТЕЛЬСТВ

В статье авторы делают акцент на глобальности проблемы преступлений в сфере компьютерной информации и компьютерных сетях. Анализируя действующее российское уголовно-процессуальное законодательство, авторы обра-

щают внимание на то, что правоохранительные органы в вопросах собирания доказательств при расследовании преступлении в сфере компьютерной информации и компьютерных сетях сталкиваются с рядом существенных трудностей и проблем. Авторами предлагаются определенные варианты решения этих проблем.

Ключевые слова: расследование, собирание доказательств, компьютерные преступления, преступлений в сфере компьютерной информации и компьютерных сетях, киберпреступления.

I.G. Smirnova
O.A. Egereva

SOME PROBLEMS ARISING IN THE INVESTIGATION OF CRIMES IN SPHERE OF COMPUTER INFORMATION SYSTEMS AND COMPUTER NETWORKS: THE FORENSIC ASPECT OF THE GATHERING OF EVIDENCE

The authors emphasize the global importance of crimes in sphere of computer information systems and computer networks. Analyzing the current Russian criminal procedural legislation of the authors pay attention to the fact that the law enforcement agencies to gather evidence in the investigation of crime in the sphere of computer information systems and computer networks are faced with a number of significant difficulties and problems. The authors offer specific solutions to these problems.

Keywords: investigation, collection of evidence, computer crimes, crimes in the field of computer information systems and computer networks, cybercrime.

Реализация предоставляемых действующим российским уголовно-процессуальным законодательством возможностей собирания доказательств при расследовании преступлении в сфере компьютерной информации и компьютерных сетях сталкивается с рядом существенных трудностей и проблем, настоятельно требующих своего решения.

Не претендуя на полноту их выявления, тем не менее, целесообразно отметить наиболее существенные и сложные из них. На наш взгляд, такими проблемами являются следующие.

Проблема розыска компьютерной информации. При раскрытии и расследовании преступлений в сфере компьютерной информации зачастую возникает необходимость в поисковой деятельности, направленной на установление (и лишь затем изъятие) компьютерной информации при наличии достаточных оснований полагать, что она имеет существенное значение для установления истины по уголовному делу [3, с. 214].

Информация по своим качественным характеристикам не совпадает ни с одним из объектов розыска. Коренное отличие состоит в ее нематериальной природе, в то время как все остальные объекты розыска материальны. Фиксируя информацию на материальном носителе, следователь изменяет форму, в которой она закреплена, но содержание остается неизменным. Следовательно, сами по себе носители не отражают никаких следов преступления и лишь с того

момента, как следователь запечатлел на них искомую информацию, приобретают процессуальную значимость. Таким образом, доказательственное значение при расследовании конкретного уголовного дела будет иметь сама информация, запечатленная на соответствующих носителях. Тем более что согласно действующему уголовно-процессуальному законодательству, следователь при производстве отдельных следственных действий может применять несколько различных способов фиксации доказательственной информации [1, с. 14].

Бурное развитие техники и использование правоохранительными органами в процессе расследования возможности высоких технологий технически позволяет «проходить» в глобальных сетях по «следам» сообщений, передаваемых по сетям электросвязи, последовательно от сервера к серверу, от компьютера к компьютеру, для их отыскания и изъятия.

Также остаются неурегулированными вопросы, касающиеся прав и законных интересов человека и гражданина при определение пределов использования розыскной деятельности сотовых систем связи, сети Интернет, спутниковой навигации, микропроцессорных устройств и других возможностей высоких технологий.

Обыск в компьютерных сетях. Сейчас компьютеры широко используются в целях обработки и хранения различного рода информации. Используются они и в преступной деятельности. В связи с этим при производстве обысков по различным категориям уголовных дел, и прежде всего при расследовании преступлений в сфере компьютерной информации, можно выделить принципиально новый объект исследования – средства компьютерной техники, а также объект поиска – информацию, хранящуюся в памяти компьютера или на внешних носителях – дисках, USB флэш-накопителях и т. п.

Не редкость, когда искомым объектом является компьютерная информация, физическое местонахождение носителей которой, по существу, не имеет какого-либо значения для следствия. В тоже время имеются достаточные основания полагать, что в определенном, удаленном массиве компьютерной информации на таком носителе находится требуемая, доступ к которой возможен с использованием сетевых технологий в условиях, когда любая задержка с ее копированием может повлечь за собой ее утрату в результате действий иных лиц, а равно иные вредные последствия. В таких условиях производство выемки компьютерной информации фактически невозможно.

В связи с этим возникает новая, на сегодняшний день законодательно не урегулированная проблема ее изъятия, а по существу – обыска в компьютерных сетях (или в среде для хранения компьютерных данных) с целью изъятия искомой компьютерной информации. Обыск должен проводиться при условии, когда примерное место ее нахождения известно. Именно это должно определять регулирование правового режима такого обыска. Учитывая особенности компьютерного пространства, настоятельно требуется отдельная уголовно-процессуальная регламентация такой деятельности [6, с. 374].

Следы в сфере компьютерной информации. Следы совершения преступления в сфере компьютерной информации в силу специфики рассматриваемого вида преступлений редко остаются в виде изменений внешней среды. Они в ос-

новном не рассматриваются современной трасологией, поскольку в большинстве случаев носят информационный характер, т. е. представляют собой те или иные изменения в компьютерной информации, имеющие форму ее уничтожения, модификации, копирования, блокирования. Как справедливо отмечает А.В. Касаткин, «при современном развитии вычислительной техники и информационных технологий «компьютерные следы» преступной деятельности имеют широкое распространение. Это должно учитываться следователями и оперативными работниками в их деятельности по собиранию доказательств наряду с поиском уже ставших традиционными следов» [7, с. 36].

Как известно, Р.С. Белкин выделяет два вида следа: след как отпечаток какого-либо объекта на другом объекте – след-отображение и след как признак некоего события – след преступления [2, с. 60].

Специфика механизма образования компьютерных следов определяется киберсредой, следообразующим объектом – программно-техническим средством, следовоспринимающим объектом – компьютерной информацией. Компьютерная информация хранится на носителях в определенной форме и может обрабатываться и преобразовываться в форму, понятную человеку, только специальными средствами компьютерной техники. В этом плане она неотделима от своего носителя.

Соответственно, следы в сфере компьютерной информации можно разделить на два типа: традиционные следы (следы-отображения, рассматриваемые трасологией, а также следы-вещества и следы-предметы) и нетрадиционные – информационные следы.

К первому типу относятся материальные следы. Ими могут являться какие-либо рукописные записи, распечатки и т. п., свидетельствующие о приготовлении и совершении преступления. Материальные следы могут остаться и на самой вычислительной технике (следы пальцев рук, микрочастицы на клавиатуре, дисководах, принтере и т. д.), а также на магнитных носителях и CD-ROM дисках.

Местонахождение информационных следов обусловлено местом совершения преступления. В этой связи, можно выделить следующие следы:

1. На носителях компьютерной информации в месте использования преступником технических средств для неправомерного доступа («рабочее место» преступника). Следы здесь обычно представлены в виде записей, которые заносятся в журналы операционной системой. Записи могут существовать как текстовые файлы или базы данных, совместимые с ODBC. Путем анализа данных следов (записей) можно получить информацию о регистрации доступа и работе пользователей, сервера, прикладных программ.

2. На промежуточных носителях компьютерной информации, посредством которых преступник осуществлял связь с компьютерной системой, подвергшейся нападению (сетевые кабели, промежуточные серверы и т. п.). Следы здесь представлены специальными техническими файлами регистрации сообщений, полиформатными записями журналов регистрации сетевых устройств и требуют специального программного обеспечения для доступа и чтения.

3. На носителях компьютерной информации, где непосредственно наступил результат неправомерного доступа (ЭВМ, подвергшаяся нападению). Обычно представлены нештатными изменениями компьютерной информации, запуском посторонних программ и процессов и т. п. [4, с. 16].

На практике серьезные проблемы может вызвать обнаружение, изъятие и фиксация материально фиксированных следов. Это связано с тем, что в большинстве случаев одним персональным компьютером может пользоваться неограниченное число пользователей. Это обстоятельство является причиной того, что на различных частях компьютера можно обнаружить большое количество отпечатков пальцев, принадлежащих нескольким людям. Как показал проведенный анализ специальной криминалистической литературы и практического опыта работников правоохранительных органов, к числу таких специфических свойств, в первую очередь, следует отнести:

– трудности в определении места происшествия и установлении его границ (в рамках которых должен проходить следственный осмотр), а также в реализации тактических рекомендаций по проведению следственного осмотра;

– необходимость активного использования специальных знаний при подготовке и проведении следственного осмотра;

– необходимость подготовки и использования специальных аппаратных и программных средств, позволяющих выявить, извлечь и зафиксировать виртуальные следы (уголовно-релевантную компьютерную информацию) [5, с. 14].

Ввиду отсутствия специализированных криминалистических средств выявления и изъятия следов неправомерного доступа к компьютерной информации в повседневной деятельности правоохранительных органов используется достаточно широкий набор стандартных программных средств общего применения, которые условно можно разделить на два основных класса: универсальные (многоцелевые) и специализированные (выполняющие определенный круг задач) программные средства.

Обозначенные проблемы требуют разработки и внесения соответствующих дополнений в действующее уголовно-процессуальное законодательство.

Одним из возможных подходов к решению этой задачи могло бы явиться включение в раздел о доказательствах УПК РФ нормы, регламентирующей порядок закрепления и изъятия следов в сфере компьютерной информации.

Подводя некоторые итоги, можно сделать выводы о том, что сложность компьютерной техники, неоднозначность квалификации, а также трудность сбора доказательственной информации не приведет в ближайшее время к появлению большого числа уголовных дел, возбужденных по ст. 272–274 УК РФ. Разработка проблемы компьютерной преступности и поиск методов борьбы с нею являются чрезвычайно важным элементом. Несмотря на то, что информационная безопасность и бюджеты на нее в России развиваются в геометрической прогрессии, количество компьютерных преступлений и инцидентов информационной безопасностью растет еще более стремительно. Остается надеяться, что законодатель будет шагать в ногу со временем и научно-техническим прогрессом, а российские криминалисты внесут свой вклад в решение проблем, касающихся преступлений в сфере компьютерной информации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Бабакова М. А. Проблема розыска при расследовании преступлений в сфере высоких технологий : автореф. дис. … канд. юрид. наук / М. А. Бабакова. – Саратов, 2010. – 24 с.

2. Белкин Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики / Р. С. Белкин. – М. : НОРМА, 2001. – 240 с.

3. Волеводз А. Г. Противодействие компьютерным преступлениям / А. Г. Волеводз. – М. : Юрлитинформ, 2002. – 496 с.

4. Иванова И. Г. Выявление и расследование неправомерного доступа к компьютерной информации : автореф. дис. … канд. юрид. наук / И. Г. Иванова. – Красноярск, 2007. – 25 с.

5. Лыткин Н. Н. Использование компьютерно-технических следов в расследовании преступлений против собственности : автореф. дис. … канд. юрид. наук / Н. Н. Лыткин. – М., 2007. – 24 с.

6. Пособие для следователя. Расследование преступлений повышенной общественной опасности / под ред. А. И. Дворкина. – М. : Лига-Разум, 1999. – 508 с.

7. Преступления в сфере компьютерной информации: квалификация и доказывание : учеб. пособие / под ред. Ю. В. Гаврилина. – М. : ЮИ МВД РФ, 2003. – 245 с.

Информация об авторах

Смирнова Ирина Георгиевна – доктор юридических наук, профессор, заведующая кафедрой криминалистики и судебных экспертиз, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, д. 11.

Егерева Олеся Александровна – кандидат юридических наук, доцент кафедры криминалистики и судебных экспертиз, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, д. 11.

Information about the authors

Smirnova Irina Georgievna – doctor of legal Sciences, Professor, head of the Department of criminology and court expertise, Baikal state University of Economics and law, 664003, Irkutsk, Lenina Ul., D. 11.

Egereva Olesya Alexandrovna – candidate of legal Sciences, the associate Professor of criminology and legal expertise of the Baikal state University of Economics and law, 664003, Irkutsk, Lenina Ul., D. 11.