УДК 343.72

В.В. Коломинов

ОСМОТР МЕСТА ПРОИСШЕСТВИЯ ПО ДЕЛАМ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В статье автор делает акцент на проблемы проведения осмотра по преступлениям в сфере компьютерной информации, необходимости использования следователем специальных знаний в области высоких технологий. Отмечает проблемы изъятия вещественных доказательств при проведении осмотра места происшествия по делам данной категории.

Ключевые слова: киберпреступность; компьютерные преступления; преступления в сфере компьютерной информации, механизм преступления.

V.V. Kolominov

THE INSPECTION OF THE SCENE OF AFFAIRS IN THE SPHERE OF COMPUTER INFORMATION

In the article the author focuses on the problems of conducting an examination of crimes in the field of computer information, the need for the investigator to use special knowledge in the field of high technologies. He notes the problems of seizure of physical evidence during the inspection of the scene for cases of this category.

Keywords: cybercrime; computer crimes; crimes in the field of computer information, the mechanism of crime.

Особое место уделяется такому следственному действию как осмотр места происшествия, особенности производства которого следует учитывать при расследовании преступлений в сфере компьютерной информации. В ходе осмотра места происшествия следователю необходимо установить, исследовать и зафиксировать обстановку места происшествия, следы преступления, преступника и иные фактические данные, позволяющие в совокупности с другими доказательствами сделать вывод о механизме преступления.

По уголовным преступлениям в сфере компьютерной информации осмотр места происшествия производится с целью выявления:

– компьютерных следов, а также их объектов – носителей (например, компьютера или системного блока, диска, дискет, флэш-накопителей и т.п.);

– традиционных (например, трасологических) следов присутствия конкретного лица на месте происшествия;

– особенностей доступа, организации, функционирования и устройства различных видов сетей, используя которые было совершено преступление.

Необходимо подвергнуть осмотру компьютерно-техническое средство и содержимое хранящихся в нем файлов. Данный осмотр следует осуществлять в рамках детального осмотра программных средств, находящихся на конкретном компьютере.

Данные действия могут затянут время осмотра и не принести необходимого результата, в виду того что следователь без специальных познаний не в состоянии обнаружить файлы, содержание которых содержит криминалистическую информацию.

С.В. Пропастин, отмечая, что когда требуется обнаружить, изъять и использовать в доказывании компьютерную информацию, находящуюся на электронном носителе, практика, использует возможности не только осмотра, но и судебной экспертизы. Однако, производство судебной экспертизы все-таки является преимущественным способом обнаружения необходимой для следствия информации. В этой связи, актуальным видится проблема разграничения возможностей осмотра и судебной экспертизы, используемых для обнаружения и исследования компьютерной информации [1, с. 129–132].

К изложенному необходимо добавить, что в памяти технически-сложного устройства, как правило, имеет место хранение телефонных номеров, смс-сообщений. В журнале вызовов можно обнаружить контакты, с которыми связывался абонент с указанием времени и продолжительности связи. Также данные устройства сохраняют информацию о соединении с глобальной сетью Интернет.

А.М. Багмет и С.Ю. Скобелин, высказывают подобные суждения, что использование электронных устройств (сотовых телефонов, смартфонов, планшетных компьютеров, портативных устройств GPS и пр.) в приготовлении, совершении преступлений, сокрытии его сле-

дов потребовало от криминалистов пересмотра современных возможностей по сбору доказательственной информации [2, с. 22–27].

В настоящее время с ее помощью следователь помимо ознакомления с журналом звонков, содержанием смс-переписок и сообщений в чатах, голосовых и видео сообщений, может также определить местонахождение интересующих следователя лиц. Такую возможность предоставляют операторы мобильной связи и непосредственное исследование технически сложного устройства.

Следователь обязан помнить о том, что на компьютерах могут быть установлены специальные защитные программы, которые без получения в определенный момент специального кода сами приступают к уничтожению информации, что возможен пароль доступа к компьютеру или к отдельным программам. При этом даже специалисту могут встретиться незнакомые, новые программно-технические средства. Целесообразно в таких ситуациях получить доступ к таким паролям и, по возможности, чтобы они были выданы добровольно. В этом случае следует определить содержание компьютерной информации, осуществить копирование документов, имеющих отношение к расследуемому мошенничеству.

Учитывая, что в соответствии с действующим законодательством изъятию подлежит только та информация, которая имеет отношение к расследуемому виду мошенничества, следователь должен определить ее содержание, а также скопировать имеющие отношение к расследуемому событию документы. Однако при отсутствии в распоряжении следователей необходимых к ее доступу паролей, или, как отмечают отдельные ученые, в связи со значительным объемом такой информации и невозможностью сразу определить, что касается расследуемого события, а что нет, следует изъять либо целиком компьютер, либо системный блок [3, с. 49].

В ходе подготовки к производству осмотра, в том числе и беседы с представителями предприятия, учреждения, организации необходимо получить первичную информацию о системах организации процесса функционирования компьютерно-технических средств, а также установить те, которые могли быть использованы в результате совершения преступлений.

На данное обстоятельство прямо указывают отдельные ученые, которые отмечают, что обязательно следует выявить администратора системы и провести его опрос. При опросе необходимо выяснить:

– какие операционные системы установлены на каждом из компьютеров;

– какое программное обеспечение используется;

– какие программы защиты и шифрования используются;

– где хранятся общие файлы данных и резервные копии;

– пароли супервизора и администраторов системы;

– имена и пароли пользователей [4, с. 147].

Во всех случаях совершения преступлений в сфере компьютерной информации при производстве осмотра места происшествия, необходимо учитывать текущее состояние компьютерно-технических средств и время, прошедшее с момента совершения преступления до момента осмотра. Такое положение обусловлено тем, что в большинстве случаев, с момента совершения преступного деяния до производства следственных действий проходит определенный (как правило, значительный) промежуток времени. В этот период может производиться: неоднократное включение и выключение компьютерно-технического средства; осуществление различных операций, в том числе, идентичных преступным действиям; использование компьютерно-технических средств значительным количеством сотрудников юридического лица и т.п. Все это ведет к потере как традиционных, так и «компьютерных» следов преступных действий мошенников.

Однако следует предполагать, что программное обеспечение, использовавшееся для совершения мошенничества в сфере компьютерной информации, вряд ли будет находиться в легкодоступных файлах, программах компьютера или сетях, а их обнаружение и выявление возможно только в ходе тщательного исследования специалистами в области компьютерных технологий.

Таким образом, осмотр места происшествия по уголовным делам о преступлениях в сфере компьютерной информации в значительной степени направлен на выявление криминалистически значимой информации, свидетельствующей о механизме преступления, возможности совершения мошенничества конкретным способом, последовательности определенных действий субъектами преступной деятельности, об установлении соответствия уже полученной информации выдвинутым версиям.

Список использованной литературы

1. Пропастин С.В. Осмотр или судебная экспертиза: выбор в пограничных ситуациях (на примере обнаружения и исследования компьютерной информации) / С.В. Пропастин // Современное право. – 2013. – № 6. – С. 129–132.

2. Волеводз А. Г. Конвенция о киберпреступности: новации правового регулирования / А. Г. Волеводз // Правовые вопросы связи. – 2007. – № 2. – С. 17–25.

3. Тропина Т. Л. Киберпреступность. Понятие, состояние, уголовно-правовые меры борьбы : монография / Т. Л. Тропина. – Владивосток, 2009.

4. Методика расследования налоговых преступлений : учеб. пособие / под общ. ред. проф. А.А. Кузнецова. – М., 2007.

5. Преступления в сфере компьютерной информации: квалификация и доказывание : учеб. пособие / под ред. Ю.В. Гаврилина. – М., 2003.

Информация об авторе

Коломинов Вячеслав Валентинович – старший преподаватель, кафедра криминалистики, судебных экспертиз и юридической психологии, Байкальский государственный университет, 664003, Российская Федерация, г. Иркутск, ул. Ленина, 11, e-mail: OffRoad88@mail.ru.

Information about the author

Kolominov, Vycheslav V. – Senior Lecturer, Chair of Criminalistics, Judicial Examinations and Legal Psychology, Baikal State University, 11 Lenin St., 664003, Irkutsk, Russian Federation; e-mail: OffRoad88@mail.ru.