Федеральное государственное казенное
образовательное учреждение высшего образования
«Дальневосточный юридический институт
Министерства внутренних дел Российской Федерации»

П. А. Жердев

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Учебное пособие

Хабаровск
ДВЮИ МВД России
2019

УДК 343.98
ББК 67.629.4
Ж591

Издается по решению редакционно-издательского совета
Дальневосточного юридического института МВД России

Рецензенты:
М. В. Старичков, начальник кафедры криминалистики
Восточно-Сибирского института МВД России, канд. юрид. наук, доц.;
Н. В. Аникаева, заместитель начальника следственного отдела
Управления на транспорте МВД России по Дальневосточному федеральному округу

Жердев, П. А.

Ж591 Расследование преступлений в сфере информационных технологий : учеб. пособие / П. А. Жердев ; Дальневост. юрид. ин-т МВД России. – Хабаровск : РИО ДВЮИ МВД России, 2019. – 76 с.
ISBN 978-5-9753-0271-7

В пособии рассматриваются технико-криминалистические особенности работы с доказательствами, представленными в электронной форме, а также даны тактические рекомендации по раскрытию и расследованию преступлений в сфере компьютерной информации и других преступлений, совершаемых с помощью средств электронно-вычислительной техники.

Издание адресовано курсантам, слушателям, адъюнктам образовательных организаций системы МВД России. Может представлять интерес для сотрудников органов внутренних дел, занимающихся расследованием преступлений в сфере информационных технологий.

УДК 343.98
ББК 629.4

ISBN 978-5-9753-0271-7

ОГЛАВЛЕНИЕ

Введение

Динамичное развитие и совершенствование компьютерных технологий, расширение функциональных возможностей технических устройств и сферы их применения, доступность информационно-вычислительной техники, кроме облегчения различных технологических и производственных процессов, способствуют появлению новых способов преступных посягательств на объекты информационно-телекоммуникационных ресурсов, а также на денежные средства, позволяющие вести расчеты безналичным путем с помощью глобальных и локальных компьютерных сетей.

Преступления, совершаемые с помощью современных информационно-коммуникационных технологий, в первую очередь посредством Интернета, мобильных средств и систем связи, представляют серьезную угрозу. Потенциал таких технологий позволяет использовать их в качестве орудий или средств совершения почти всех известных уголовному законодательству преступлений, таких как:

1) экономические преступления (налоговые преступления, незаконное предпринимательство и др.);

2) преступления, связанные с блокировкой информации (DoS-атака[1], блокирование сайтов, серверов, компьютеров частных лиц и организаций);

3) преступления, связанные с хищением денежных средств с банковских карт, счетов граждан и организаций (скимминг[2], фишинг[3], распространение вредоносного программного обеспечения, кардинг[4] в системах дистанционного банковского обслуживания);

4) преступления, связанные с распространением и пропагандой идеологии фашизма, экстремизма, терроризма и сепаратизма;

5) преступления, связанные с незаконным оборотом оружия и наркотических средств;

6) преступления, связанные с подделкой документов, изготовлением поддельных денежных билетов, документов и ценных бумаг;

---

[1] *DoS-атака* (*DoS* – от англ. *Denial of Service* – «отказ в обслуживании») – хакерская атака на вычислительную систему с целью довести ее до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам) либо этот доступ будет затруднен.

[2] *Скимминг* (от англ. *skim* – «снимать сливки») – копирование данных платежной карты с помощью специального устройства (скиммера). Данные карты считываются, когда владелец вставляет ее в банкомат. Для получения PIN-кода злоумышленники устанавливают мини-камеры или накладки на клавиатуру.

[3] *Фишинг* (транскрипция англ. *phishing*, произошедшего от *fishing* «рыбная ловля, выуживание») – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Это достигается за счет массовой рассылки электронных писем якобы от имени популярных брендов или личных сообщений в социальных сетях и т. п., например, от имени банка.

[4] *Кардинг* (транскрипция англ. *carding* – «чесание») – мошенничество с кредитной (платежной) картой, при котором производится операция с использованием этой карты или ее реквизитов, не инициированная или не подтвержденная ее держателем.

7) преступления против половой неприкосновенности (распространение порнографии, вовлечение малолетних в занятие проституцией);

8) распространение вредоносного программного обеспечения;

9) общеуголовные преступления (кража, убийство, мошенничество, вымогательство, совершенные с использованием электронно-вычислительных средств и технологий).

В настоящее время преступления в сфере компьютерной информации хотя и имеют незначительный удельный вес в общей структуре преступности (в сравнении с другими преступлениями), однако их число ежегодно растет. Наиболее частыми видами преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий, по-прежнему остаются мошенничество и кража денежных средств со счетов граждан и организаций, так как позволяют преступникам получать прибыль. Это дает основания говорить о хищении с помощью компьютерной техники как о самостоятельном объекте изучения частной криминалистической методики расследования преступлений, совершаемых в сфере информационных технологий.

При совершении преступлений в сфере информационных технологий используются последние достижения научно-технического прогресса, что усложняет процесс раскрытия и расследования уголовных дел данной категории, а сотрудники оперативных подразделений часто не имеют представления о сфере, в которой совершено преступление, не знают алгоритма действий при проверке заявлений и сообщений о преступлениях, в частности того, какие именно оперативно-разыскные мероприятия и следственные действия необходимо провести для обнаружения и фиксации следов и обстоятельств, при которых было совершено противоправное деяние. Более того, от способа совершения конкретного преступления зависят ход расследования, степень организованности взаимодействия, алгоритм и очередность действий уголовно-процессуального характера.

Для того чтобы частная криминалистическая методика в достаточной степени удовлетворяла потребностям судебно-следственной практики, она должна иметь высокую степень теоретической обоснованности. Научной базой являются криминалистические знания, а также знания в области смежных наук: уголовного права, уголовного процесса, оперативно-разыскной деятельности органов внутренних дел, информатики и информационных технологий в профессиональной деятельности.

Указанные обстоятельства диктуют необходимость углубленного изучения существующих проблем для выработки эффективных способов противодействия преступности в данной сфере.

ГЛАВА 1. ОСОБЕННОСТИ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ И ЕЕ РОЛЬ В ФОРМИРОВАНИИ РЕКОМЕНДАЦИЙ ПО РАССЛЕДОВАНИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Понятие, сущность, значение криминалистической характеристики и обстоятельства, подлежащие установлению и доказыванию в процессе расследования преступлений, совершаемых в сфере информационных технологий. Качественные и количественные показатели киберпреступности

В результате научно-технического прогресса сегодня люди все больше используют в повседневной жизни различные медиаустройства и компьютеры. Преступники также все чаще применяют высокотехнологичное оборудование – в качестве средств и орудий преступления.

Существующие в настоящее время технологии позволяют совершать преступления в любой точке мира, не находясь в ней, получать сведения и осуществлять противоправные действия анонимно.

Сервисы мгновенной отправки сообщений и электронной почты создают условия для практически беспрепятственного общения преступников с потенциальными жертвами и между собой.

Компьютеры и другие медиаустройства могут стать средством доступа в базы данных федеральных органов исполнительной власти, а могут стать источником сведений о преступлении такого или иного рода, лицах, его совершивших, и лицах, в результате него пострадавших.

Представляется, что **основным техническим средством совершения преступлений в сети Интернет** служит персональный компьютер, который позволяет упростить противоправные действия и сохранить их конфиденциальность.

Применение телекоммуникационных средств связи оказало влияние на появление нового структурного элемента организованной преступности – киберпреступности, с образованием которого повысился уровень криминализации современного российского общества.

К настоящему времени информационный процесс прошел несколько эволюционных этапов, смена которых определялась главным образом развитием научно-технического прогресса и появлением новых технических средств переработки информации, функционирующих на базе микропроцессорной техники, а также современных средств и систем телекоммуникаций информационного обмена, аудио-, видеотехники и т. п., обеспечивающих проведение операций по сбору, продуцированию, накоплению, хранению, обработке, передаче информации [73, с. 104].

Чаще всего **предметом преступного посягательства** при совершении преступлений в сфере компьютерной информации выступает «охраняемая законом компьютерная информация» [3, ст. 272]. Как отдельная категория предмета преступного посягательства эти сведения наделяются специальным режимом

государственно-правового регулирования, и в зависимости от порядка предоставления или распространения делятся:

1) на информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит распространению или предоставлению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается (например, информация, отнесенная к государственной, служебной, коммерческой, банковской тайне; персональные данные и т. п.).

Вопрос отнесения какой-либо информации к «охраняемой законом» связан прежде всего с определением совокупности общественных отношений, которые регулируют права и интересы обладателя ценной информации, предупреждая ее недозволенное распространение третьим лицам.

Опираясь на определения ученых [См., например: 58, с. 52], можно определить *охраняемую законом компьютерную информацию* как компьютерную информацию, для которой непосредственно законом или ее обладателем, которому законом предоставлено такое полномочие, установлен специальный режим доступа для определенного круга лиц.

Как известно, предмет преступного посягательства и средства совершения преступления, наряду с рядом других элементов, входят в криминалистическую характеристику преступления.

Далее мы рассмотрим не все элементы такой характеристики, а *только наиболее значимые для раскрытия преступлений в сфере информационных технологий и в то же время «проблемные»* – те, которые сложно установить, но это необходимо для расследования.

Анализ практики раскрытия и расследования преступлений в сфере информационных технологий позволяет выделить в качестве таких место совершения преступления, особенности личности обвиняемого, которые мы рассмотрим в данном параграфе; способы подготовки, совершения, сокрытия следов преступления и механизм следообразования, о которых пойдет речь в следующих параграфах данной главы.

Прежде всего, следует отметить, что *криминалистическая характеристика* – это научная категория, которая определяется системой взаимосвязанных, взаимообусловленных элементов, позволяющих следователю эффективно организовать процесс [15, ст. 103]. Основные ее составляющие – предмет преступного посягательства; обстановка совершения преступления, включающая в себя место, время и др.; сведения о способах подготовки, совершения, сокрытия преступления; сведения о типичных механизмах следообразования, а также о личности преступника и потерпевшего.

Ряд этих элементов, например событие преступления (время, место, способ и другие обстоятельства совершения преступления), обстоятельства, характеризующие личность обвиняемого, согласно УПК РФ, относятся также к обстоятельствам, подлежащим доказыванию при производстве по уголовному делу [2, ст. 73].

Анализ следственной и судебной практики показывает, что значительную сложность при раскрытии и расследовании преступлений с использованием компьютерной техники представляет установление такого элемента события преступления, как **место совершения преступления**.

В криминалистике традиционно используют ряд терминов. Так, *местом преступления* считается место, где определенным способом было совершено преступление, – участок местности или помещение, где произошло противоправное деяние [15, с. 115]. Под *местом происшествия* понимают участок местности или помещение, где имеются следы расследуемого события [15, с. 115].

Когда идет речь о преступлениях в сфере информационных технологий, более точным нам кажется термин «*место совершения преступления*», который понимается нами широко, объединяя и место преступления, и место происшествия. Именно место совершения преступления как элемент криминалистической характеристики обладает существенной информативностью, ведь оно оказывает влияние на весь процесс формирования следовой картины и является «носителем» как материальных, так и идеальных следов.

Определяющее значение имеют признаки и свойства места совершения преступления в сфере информационных технологий. Это обусловлено прежде всего спецификой электронной информации, которая подлежит обработке, хранению, обмену, а для этого необходимо наличие компьютерных средств и средств обмена, то есть сети, в частности сети Интернет.

Существует мнение, что система функционирования компьютерных сетей создавалась для контроля процесса перемещения информации внутри нее, а также для установления источников ее происхождения и конечных потребителей. Это, с одной стороны, приводит к нарушению законных прав и интересов гражданина, а с другой – позволяет выявлять, раскрывать, расследовать преступления, совершаемые в сфере компьютерной информации.

Возможность контроля движения информации заключается, по мнению И. Н. Воробца, в том, что система адресации в сети Интернет, описываемая IP-протоколом, построена на основе присвоения каждому компьютеру, подключенному к сети, уникального идентификационного номера – IP-адреса[5] [55, с. 71].

Имеется *ряд проблем, препятствующих определению места совершения преступления*, а равно расследованию. Например, спамеры[6], как правило, используют электронные адреса вне доменной зоны .ru[7], что затрудняет своевременное получение сведений о месте нахождения таких IP-адресов. Так, потерпевший обращается в отдел полиции по месту жительства, где и должна проводиться проверка сообщения о преступлении, а субъекты преступления могут

[5] *IP-адрес* – это набор из четырех десятичных чисел, разделенных точками. Подробнее об этом понятии см. в § 3 гл. 1.

[6] *Спамер* – распространитель спама. *Спам* (англ. spam) – массовая рассылка электронных писем и иной корреспонденции рекламного характера лицам, не выражавшим желания ее получать.

[7] *Доменная зона* – вторая часть доменного имени (уникального названия узла в Интернете), стоящая после точки, например: .ru (российский национальный домен верхнего уровня), .su, .com и др.

проживать в другом месте, в другой части страны, мира, следовательно, и следы минимальны, ведь кроме сведений из компьютера потерпевшего собрать какие-либо данные не представляется возможным [28, с. 141].

Изучив особенности функционирования компьютерной сети, можно сделать вывод, что, с одной стороны, *местом совершения преступлений в сфере компьютерной информации является* сама информационно-телекоммуникационная сеть, в которой и происходит ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки, передачи компьютерной информации; а с другой стороны, место совершения указанного преступления – место нахождения конкретного компьютера, с которого осуществляется неправомерный доступ, ведь именно в этом месте содержится основная информация о других элементах криминалистической характеристики преступления: способах его подготовки, совершения и сокрытия следов.

Кроме того, совершение преступлений с использованием средств электронно-вычислительной техники предусматривает наличие нескольких устройств, участвующих в процессе обмена информацией, при этом между ними может быть большое расстояние. Такое обстоятельство затрудняет процесс выявления, раскрытия, расследования преступлений в сфере компьютерной информации, в частности, когда неправомерный доступ осуществляется из-за рубежа. Таким образом, сложно окончательно определить место совершения изучаемого противоправного деяния, что обусловлено его двойственным объектом. «Преступное деяние, – как отмечает в этой связи Н. А. Колоколов, – считается законченным с момента получения виновным суммы денег (чужого имущества), а равно приобретения им юридического права на распоряжение такими деньгами (имуществом). А факт ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки и передачи информации в зависимости от обстоятельств может содержать признаки приготовления» [61, с. 10].

Базисной составляющей **личности преступника** обычно являются знания, а также умения и навыки работы с компьютерными системами.

Потерпевшим может стать как рядовой пользователь компьютерной сети, так и определенный человек, обладающий в силу различных обстоятельств значимой для преступника информацией.

Лиц, совершающих преступления в сфере информационных технологий, *по возрастному критерию* следует разделить на две группы.

Первая категория – люди 18–25 лет. Это, как правило, студенты средних или высших технических учебных заведений, обучающиеся по специальностям типа «Инфокоммуникационные технологии и системы связи», «Эксплуатация электронно-вычислительных машин» и др. Они имеют определенные познания в сфере создания, развития и использования информационных систем, вследствие чего, в поисках путей самовыражения, «погружаются» в компьютерные сети в целях развлечения, хулиганства или наживы.

На то, что преступник относится к данной категории, могут указывать следующие особенности:

– преступление было совершено в отношении геймера[8], который за деньги хотел «купить улучшения» для успешного прохождения браузерной онлайн-игры;

– использовалась вредоносная программа, чит-программа для взлома компьютерной игры, получения ключей доступа;

– преступление не было продуманным, длительная подготовка к нему не велась (средство совершения, как правило, домашний компьютер или компьютер знакомого);

– меры для сокрытия следов преступления не принимались.

Вторая группа – от 25 лет. Это уже вполне сформировавшиеся личности, обладающие высокими профессиональными навыками и устойчивыми преступными связями, а также определенным жизненным опытом, в том числе высококвалифицированные специалисты с высшим математическим, инженерно-техническим или экономическим образованием.

Особенности совершения преступлений данной группой:

– деяния носят осознанный корыстный характер (получение прибыли, вымогательство или кража);

– преступления совершаются организованной преступной группой, действующей на территории одной страны, или преступным сообществом, имеющим межрегиональные и международные связи;

– преступления характеризуются серийностью, многоэпизодностью;

– обязательно принимаются меры по конспирации участников группы: сокрытие способов, средств и методов удаленного доступа к интернет-ресурсам жертвы);

– высока техническая оснащенность.

Изучение разными авторами судебной практики, в первую очередь зарубежной, по данной категории дел показало, что *образовательный уровень лиц, совершающих преступления в сфере компьютерной информации*, не только выше, чем образовательный уровень лиц, совершающих иные преступления, но в некоторых случаях даже значительно превышает средний образовательный уровень населения. Более того, в юридической литературе [См., например: 18, с. 136] отмечают постоянно возрастающий криминальный профессионализм и обеспеченность современной техникой лиц, совершающих преступления в сфере информационных технологий.

Представляется, что не является исключением и ситуация в России. Таким образом, отечественными специалистами делается правомерный, на наш взгляд, вывод о том, что российские организации, компании и фирмы еще длительное время будут оставаться весьма уязвимыми с точки зрения неправомерного доступа к своим информационным ресурсам [16, с. 12].

Еще в 1987 г. Ю. М. Батурин писал, что «мафия... нуждается в компьютерах...» [13, с. 27]. Это подтверждает и исследование, проведенное В. Б. Веховым: *основная часть преступлений в сфере компьютерной информации совершается в составе преступных групп* [1718]. Прямую связь компьютерной преступности

[8] *Геймер* – человек, играющий в видеоигры.

с организованной преступностью отмечают в своих работах Е. П. Ищенко [28], Н. Г. Шурухнов [40], В. Б. Вехов [18] и другие ученые.

Отечественные криминалисты, изучающие проблемы борьбы с организованной преступностью, считают, что преступления в сфере информационных технологий в Российской Федерации наиболее часто совершаются в области экономики и участвуют в них организованные преступные группы. За короткий период времени разрозненные группы сумели пройти путь до интеллектуально и технически обеспеченных, хорошо законспирированных преступных сообществ. В связи с этим правильно связывать компьютерную преступность с организованной преступностью, как это делает ряд российских исследователей [72, с. 3].

Преступность, в том числе и в сфере информационных технологий, как любая разновидность негативных социальных явлений, **нуждается в установлении причин и условий, ей способствующих, в определении количественных и качественных характеристик.**

Основными *факторами распространения преступности* в сфере компьютерной безопасности являются:

– высокий ущерб. В настоящее время организованные преступные группы все чаще пользуются современными информационными технологиями, применяют вычислительную и другую электронную технику для хищения крупных денежных средств со счетов банковских учреждений;

– высокий уровень латентности;

– возможность совершать компьютерные преступления на расстоянии, иногда даже с другого континента;

– участие организованных преступных групп и преступных транснациональных формирований[9];

– скоротечность реализации преступного замысла и получение прибыли. Несанкционированный доступ часто осуществляется в течение короткого промежутка времени, который может исчисляться секундами;

– несовершенство законодательной базы. В области информационно-обрабатывающих технологий законодательство часто не поспевает за развитием техники, а подготовка сотрудников правоохранительных органов является недостаточной для решения задач, связанных с обнаружением и контролем за этим новым видом преступности;

---

[9] Хакерская группировка Anonymous во время арабских революций в 2010–2011 гг. совершила ряд атак на интернет-сайты государственных органов власти Египта, интернет-ресурсы Министерства информации, а также правившей на тот момент национальной демократической партии. Вследствие этого правительство Египта вынуждено было отключить Интернет по всей стране. В результате пятидневной блокады Сети страна потеряла около 90 млн долларов США. Кроме египетских хакеры «Anonymous» взломали сайты 70 американских государственных учреждений. Преступники мстили за своих арестованных соучастников крупным предприятиям вроде SONY и FBI, угрожали опубликовать секретные данные офицеров полиции в случае отказа от освобождения их соратников.

Организация Североатлантического договора (НАТО) причислила хакерскую группировку Anonymous к главным врагам международного военного блока, среди которых значились террористическая группировка «Талибан» и «Северная Корея» [Приводится по: 28, с. 196].

– сложность установления факта совершения преступления. Часто преступники прибегают к различным уловкам, маскируют преступные деяния, объясняя действия многочисленными объективными и субъективными причинами, которые могут иметь место в действительности (например, сбоем в работе программного обеспечения, выходом из строя периферийного оборудования или какого-либо электронного устройства, входящего в состав электронно-вычислительной техники);

– сложность идентификации преступника;

– сложность обнаружения, сбора и юридического закрепления доказательств совершения компьютерного преступления;

– специфика субъекта преступления: чаще всего, как мы уже рассмотрели, им является высокоинтеллектуальная личность, профессионал в области информационных технологий [57, с. 31].

По оценкам специалистов, преступления в сфере компьютерной информации во всем мире, в том числе и в России, характеризуются высоким уровнем латентности и динамичностью. По темпам роста преступления в сфере компьютерной безопасности заметно выделяются среди других общественно опасных деяний. До последнего времени удельный вес преступлений в сфере компьютерной информации в России был невысок, что давало основание говорить о «младенческом возрасте» данного вида преступности.

Ежегодно на территории страны фиксируется *достаточно большое число преступлений в сфере компьютерной информации*. Например, по ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» в 2018 г. их количество составило 1761, в 2017 г. – 1079, в 2016 г. – 994, в 2015 г. – 1396. На территории Дальневосточного федерального округа в 2018 г. было зафиксировано 91 преступление, в 2017 г. – 67 преступлений, в 2016 г. – 22, в 2015 г. – 48 [11].

Поэтому представляется вполне обоснованным вывод о том, что ни один вид преступлений не имеет столь *высокой динамики развития и уровня латентности*, как преступления в сфере компьютерной информации.

Говоря о проблеме латентности, не следует забывать, что она самым тесным образом связана и с объективными возможностями правоохранительной системы. Чем более ограничены возможности правоохранительных органов, тем более значительная часть преступлений данного вида остается «в тени», со всеми вытекающими отсюда социальными последствиями.

В связи с исследованием проблемы раскрытия компьютерных преступлений, целесообразно, на наш взгляд, коснуться и *проблемы профилактики*. В. В. Крылов приводит данные совместного исследования Института компьютерной безопасности и ФБР, в котором приняли участие представители крупнейших западных компаний. Из опросов респондентов следует вывод о весьма высокой уязвимости западных компаний и фирм:

– 50 % респондентов отметили, что их фирмы не имеют плана действий на случай несанкционированного вторжения;

– 70 % респондентов указали, что не имеют специальных технических средств, предупреждающих о вторжении в их информационные системы;

– в подавляющем большинстве случаев сотрудники безопасности организаций даже не имеют представления о существующих способах и методах проникновения в их защищенную компьютерную среду. При этом в информационной системе нередко хранится ценная информация [29, с. 42].

Кратко подводя **итог изложенному** в данном параграфе, отметим:

1) *информационные технологии* – это приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных [5], иными словами – это совокупность методов, способов и технических средств сбора, организации, накопления, хранения, поиска, обработки, передачи и представления информации, расширяющих знания людей и развивающих их возможности по управлению техническими и социальными процессами;

2) *компьютерная информация* – это сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов;

3) объектом преступлений в сфере компьютерной информации выступают общественные отношения в сфере обеспечения безопасности охраняемой законом компьютерной информации;

4) на структуру и содержание криминалистической характеристики существенное влияние оказывают уголовно-правовые особенности преступлений в сфере компьютерной информации;

5) данные, составляющие криминалистическую характеристику противоправных деяний, совершенных с помощью компьютерной техники, позволяют определить правильные направления в расследовании, особенно на первоначальном этапе, в условиях дефицита информации;

6) вызывающими сложности при установлении и в то же время значимыми элементами криминалистической характеристики преступлений в сфере компьютерной информации выступают место совершения преступления, особенности личности преступника, способы его подготовки, совершения и сокрытия.

7) вопрос о том, что считать местом совершения преступления, не решен однозначно, но, опираясь на практику расследования, можем сделать вывод, что место нахождения материальных следов (конкретное помещение, где был компьютер, с которого осуществлялся незаконный доступ) скорее всего и является местом совершения преступления в сфере компьютерной информации;

8) основная часть преступлений в сфере компьютерной информации совершается в составе преступных групп; преступления в сфере информационных технологий имеют высокий уровень латентности.

§ 2. Способы подготовки к совершению, совершения преступлений в сфере информационных технологий и сокрытия их следов как элемент криминалистической характеристики

Одним из базовых элементов криминалистической характеристики преступлений в сфере информационных технологий является способ совершения преступления, поэтому предлагаем рассмотреть этот вопрос отдельно.

В толковом словаре русского языка С. И. Ожегова **понятие «способ»** определяется как «действие или система действий, применяемых при исполнении какой-либо работы, при осуществлении чего-нибудь» [37, с. 674]. В научных же кругах определение остается дискуссионным, поскольку его толкуют как в широком, так и в узком смысле.

В узком смысле о способе принято говорить, как, во-первых, о приемах, методах, тактических средствах, применяемых для совершения преступления, а во-вторых, о тех методах и приемах, которые использует преступник для совершения преступления [67, с. 90].

В широком смысле способом совершения преступления признается деятельность преступника, детерминированная психофизическими свойствами личности и условиями внешней среды, включающая в себя подготовку, совершение и сокрытие противоправного деяния, а также выбор преступником места, времени, орудий и средств, условий, соответствующих цели совершаемых им действий [62, с. 145].

Необходимо отметить, что сведения о способе совершения преступления в сфере компьютерной информации позволяют выдвигать следственные версии как о характере совершенного противоправного деяния, так и о субъекте преступления.

В криминалистической науке *способ совершения преступления* определяют как «объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения им преступления, оставляющую характерные следы вовне, позволяющие с помощью криминалистических приемов и средств получить представление о сути произошедшего события, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и, соответственно, определить оптимальные методы решения задач раскрытия и расследования преступления» [45, с. 127].

Таким образом, рассматриваемый элемент криминалистической характеристики состоит из системы деяний преступника по подготовке, непосредственному совершению и сокрытию преступления.

Способы подготовки к совершению преступления в сфере информационных технологий разнообразны. Это может быть написание, тестирование специальных компьютерных программ для взлома, а также внедрение вредоносных программ, программ-шпионов, поиск паролей, определение способов беспарольного входа в локальную или глобальную сеть и др. Все это оставляет виртуальные следы как в компьютере преступника, так и в компьютере потерпевшего.

Как верно отмечает А. Смушкин, для указанных преступных действий могут использоваться программы различного уровня сложности: стандартные – которые составлены максимально просто и которые легко найти в Интернете или

в специальной области закрытого участка Интернета; приспособленные – переделанные самим злоумышленником под свои нужды; самостоятельно написанные им [78, с. 44].

Совершение преступления определенным способом отражается во внешней обстановке, оставляет следы, которые входят в информационную модель преступления. Как отмечают В. Б. Вехов и С. А. Ковалев под *типовой информационной моделью преступления в сфере компьютерной информации* следует понимать информационную систему, построенную на основе статистической обработки репрезентативной выборки уголовных дел о преступных посягательствах названного вида, которая отражает закономерные связи между типичными элементами события преступления, используется для построения типовых версий, а также формирования методики расследования данной категории преступлений [19, с. 12].

Способы совершения преступлений в сфере информационных технологий (компьютерной информации) конкретны и имеют *ряд признаков*, понимание которых имеет важное значение при их раскрытии и расследовании. К таким признакам можно отнести сведения:

– о распространенности данного способа;

– о конкретных приемах его применения;

– об используемых при этом технических и иных средствах (орудиях преступления) и о возможных источниках их получения (доступа к ним): данные о конструктивных особенностях, о том, какие технологические процессы, оборудование, материалы использовались для их изготовления; как они применялись при совершении преступления; о недостатках в учете и хранении, которые облегчили доступ к ним преступников, и др.;

– о методах подготовки преступления и т. д. [18, с. 146].

Преступления в сфере компьютерной информации могут совершаться множеством способов. Более того, научный прогресс в сфере информационных технологий приводит к постоянному росту их числа. Поэтому *достаточно сложно перечислить все способы и более целесообразно систематизировать их, объединив в определенные группы.*

Прежде всего, представляется целесообразным обобщение способов совершения компьютерных преступлений, предложенное В. Б. Веховым, В. В. Поповой и Д. А. Илюшиным, **на основании такого классификационного критерия как метод, применяемый преступником для осуществления целенаправленного воздействия на средство электронно-вычислительной техники и компьютерную информацию**.

Предложенная указанными авторами классификация выглядит следующим образом:

1) непосредственный доступ к электронным носителям и средствам компьютерной техники, содержащим в памяти охраняемую законом информацию;

2) дистанционный (удаленный или администрированный) доступ к электронным носителям и охраняемой законом компьютерной информации;

3) фальсификация входных (выходных) данных и управляющих команд;

4) несанкционированное внесение изменений в существующие компьютерные программы и создание вредоносных программных средств;

5) незаконное распространение электронных носителей, содержащих охраняемую законом компьютерную информацию;

6) комплексные способы [20, с. 30].

К первой группе относится *неправомерный непосредственный доступ к объектам компьютерной информации, содержащейся в их памяти, для ее уничтожения, модификации, блокирования либо копирования*.

Это условно называемые традиционными методы получения доступа к электронным носителям и средствам компьютерной техники как к чужому имуществу, то есть разновидности преступлений против собственности.

Наиболее распространены такие:

– постоянное или временное изъятие объектов путем кражи, мошенничества (обман, введение в заблуждение под, на первый взгляд, достоверным предлогом), грабежа и разбоя;

– обращение их в свою пользу или в пользу других лиц.

Специфичными следами применения этих способов выступают:

– следы орудий взлома и инструментов;

– одорологические следы;

– следы повреждения, уничтожения и (или) модификации охранных (сигнальных) устройств, а также замков и запирающих механизмов;

– показания автоматизированных систем охраны и контроля доступа в помещение, где находятся средства компьютерной техники и (или) электронные носители информации, например, фото- или видеодокументы из систем охранного видеонаблюдения;

– следы пальцев рук на средствах компьютерной техники, охранных и сигнальных устройствах, на их клавиатуре, соединительных и электропитающих проводах и разъемах, розетках и штепсельных вилках, тумблерах, кнопках и рубильниках, включающих средства компьютерной техники и электрооборудование;

– остатки соединительных проводов и изоляционных материалов, капли припоя, канифоли или флюса;

– следы проплавления, прокола, надреза изоляции проводов средств компьютерной техники, наличие участков механического сдавливания и приклеивания сторонних предметов;

– следы фальсификации первичных документов, отражающих движение машинных носителей информации[10] и документированной компьютерной информации, а также операции, произведенные с их помощью.

Ко второй группе способов относятся те, которые основаны на *применении средств дистанционного доступа к электронным носителям информации и охраняемой законом компьютерной информации*.

[10] *Машинный носитель информации* – материальный носитель информации, предназначенный для записи, хранения и воспроизведения компьютерной информации средствами вычислительной техники, а также сопрягаемыми с ними устройствами.

Типичными орудиями совершения преступления являются:

– специальные технические средства, предназначенные (разработанные, приспособленные, запрограммированные) для негласного дистанционного копирования, модификации, блокирования и уничтожения компьютерной информации с технических устройств, ее обработки и передачи;

– вредоносные программы;

– специальные программно-технические средства подбора пароля (кода доступа) к охраняемой компьютерной информации (код-грабберы и генераторы паролей);

– средства электросвязи;

– компьютеры со стандартным программным обеспечением и промежуточные (транзитные) машинные носители информации.

В юридической литературе способы совершения преступлений в сфере компьютерной информации рассматриваемой группы часто связывают с понятием «телекоммуникационный доступ», так как они невозможны без установки временного или использования постоянно существующего канала электросвязи. Таким образом, неправомерные действия осуществляются через промежуточные (транзитные) электронные носители информации и средства электросвязи [31, с. 214].

Неправомерный доступ к компьютерной информации с применением способа, относящегося ко второй группе, можно рассмотреть на примере материалов следующего уголовного дела.

> Гражданин П. 26 августа 2014 г., обладая достаточными познаниями в области компьютерной техники и навыками работы с компьютерными программами, предназначенными для удаленного доступа и подключения к сетевым ресурсам, находясь на территории г. Хабаровска, с целью реализации преступного умысла, осознавая, что в связи с его предстоящим увольнением прямой доступ к сетевой инфраструктуре ему будет запрещен, используя свою доменную учетную запись, предпринял действия для получения неправомерного доступа к охраняемой законом компьютерной информации, размещенной на серверах организации, для чего установил программное обеспечение удаленного доступа «Ammyy Admin», которое позволяет осуществлять удаленное управление серверами без присутствия человека за компьютером, на сервер «1С», файл сохранил в директории «C:\zbx\dev» и переименовал в файл «az» чтобы скрыть, что на сервере «1С» находится программа удаленного доступа.
>
> В дальнейшем П., в нарушение требования Закона Российской Федерации «Об информации, информационных технологиях и о защите информации», согласно которому информация конфиденциального характера может быть использована только ее правообладателем, с целью уничтожения данных, хранящихся на серверах, и приостановления работоспособности организации, используя программное обеспечение «Ammyy Admin», через устройство с IP-адресом, зная особенности и пароли сетевой инфраструктуры, в том числе системы хранения данных, источников бесперебойного питания, так как ранее являлся руководителем инженерного отдела организации, осуществил неправомерный доступ к охраняемой законом компьютерной информации, содержавшейся на серверах.

Его умышленные действия привели 28 декабря 2014 г. к повреждению программного обеспечения и безвозвратному уничтожению следующих сведений организации:

– информации о хозяйственно-финансовых отношениях с контрагентами;

– данных об объеме и повторяемости (периодичности) товарооборота с деловыми партнерами;

– конфиденциальной информации об адресах мест жительства (участков мест нахождения) служащих, их паспортных данных, персональных данных;

– финансовых показателей деятельности, финансовой, бухгалтерской и налоговой отчетности, сведений финансового, бухгалтерского и налогового учета;

– информации, поступившей по электронной почте на электронный адрес общества и электронные адреса работников, информации, отправленной по электронной почте с электронного адреса организации и электронных адресов сотрудников;

– резервных копий баз данных «1С», почтового сервера проектов компании базы данных программистов.

Это повлекло причинение крупного ущерба на общую сумму 1 469 062 рублей» [8].

Пример наглядно демонстрирует возможность нанесения крупного ущерба в результате неправомерного доступа к охраняемой законом информации и воздействия на нее путем ввода, копирования, модификации или удаления отдельных ее элементов.

Типичными следами преступлений второй группы являются:

1) сведения регистрирующей (мониторинговой) аппаратуры:

– радиосканирующих и пеленгующих приборов, устройств, компьютеризированных анализаторов проводных сеток сетей электросвязи;

– программно-технических средств обороны защиты портов компьютера – рабочих станций компьютерной сети;

– аппаратуры контроля и регистрации соединений абонентов в сети электросвязи;

– специализированных программ для компьютера – антивирусов;

2) наличие на месте происшествия:

– орудий преступления либо или их частей;

– методической литературы, видеодокументов, отдельных их фрагментов, описывающих технологию создания и/или применения средств преступления;

– машинных носителей с компьютерной информацией, к которой был незаконный доступ, либо иных материальных носителей с ее производными.

К третьей группе относятся *способы, базирующиеся на фальсификации (модификации) входных (выходных) сведений и управляющих команд*.

Они характерны для экономических преступлений, в частности для хищения денежных средств и иных преступных посягательств, когда подменяются входные и/или выходные данные бухгалтерского учета в ходе автоматизированной обработки документов, ведется так называемая двойная (черная) бухгалтерия.

Такие способы преступники выбирают, как правило, в тех ситуациях, когда принимаемые меры защиты информации не соответствуют установленным законам и правилам ее сохранности. Так, отсутствие должного контроля со стороны администрации и службы безопасности организации за деятельностью сотрудников позволяет злоумышленникам в корыстных целях фальсифицировать сведения, отраженные на электронных носителях и в документах, полученных по каналам электросвязи [54, с. 78].

Типичные следы можно обнаружить путем сравнения конечных сведений и данных, содержащихся в первичных документах, на основе которых формируется электронный документ и электронная защита.

Четвертая группа – это *несанкционированное внесение изменений в существующие программы для компьютеров и создание вредоносных программных средств*, результатом чего выступают блокирование, уничтожение, копирование или модификация информации, нарушение общей работы компьютера.

Типичные следы:

– сбой в работе программы;

– нарушение работы компьютера, системы компьютера, сети и периферийного оборудования, управляемого компьютером;

– уничтожение, блокирование, модификация или копирование информации конкретного вида;

– несанкционированное изменение места расположения различных файлов (папок – директорий) и (или) программ для компьютера дополнительно на машинном носителе информации;

– появление в памяти компьютерного устройства или на электронном носителе новой информации (файлов, приложений программ, директорий), происхождение которых неизвестно;

– показания тестирующих (специальных антивирусных программ защиты от несанкционированного доступа) и мониторинговых приложений и программ для компьютера;

– расхождение контрольных данных, отраженных в журнале оператора (администратора сети) компьютера, с фактическими, оказавшимися в нем.

К *пятой группе способов* относятся действия субъекта, выражающиеся в *незаконном распространении электронных носителей, содержащих охраняемую законом компьютерную информацию либо сведения, распространение (оборот) которых запрещен уголовным законодательством*.

Типичные следы преступлений этой группы:

– следы пальцев рук подозреваемого, биологические следы и микрообъекты, обнаруженные на персональных компьютерах, ноутбуках, серверах, смартфонах, роутерах, внешних электронных носителях, иных устройствах (видеорегистраторах, игровых приставках и др.);

– наличие файлов компиляторов[11];

[11] *Компилятор* – специальная программа, которая переводит текст программы, написанный на языке программирования, в набор машинных кодов;

– модификация информации в виде частичной декомпиляции[12] программы для достижения способности к взаимодействию с другими программами;

– следы подделки и исправления в документах и лицензионных договорах на использование и распространение программных продуктов;

– нарушение аппаратной системы защиты информации, признаки воздействия на вычислительную технику.

Шестая группа – комплексные способы совершения преступлений в сфере информационных технологий – предполагает применение преступником двух и более способов из различных групп, причем один из них всегда используется как основной, а другие выступают как вспомогательные и могут быть направлены, например, на сокрытие следов преступления [53, с. 30].

Если рассматривать **способы совершения преступлений в сфере информационных технологий с учетом такого классификационного критерия, как новизна, нетрадиционность**, то можно выделить как особые виды, которые могут быть одними из способов в ряду комплексных, еще два.

Совершение преступлений с использованием криптовалюты характерно в первую очередь для участников организованных преступных групп и сообществ общеуголовной и экономической направленности и связано с незаконным оборотом запрещенных товаров и услуг, когда в качестве средств для оплаты используются электронные платежные единицы цифровой валюты [69, с. 90] (криптовалюты), одним из наиболее популярных видов которой является биткойн (биткоин).

Вкладывая «криминальные» деньги в привлечение и функционирование цифровой валюты, преступные формирования нередко становятся технологически недосягаемыми для государственных контролирующих органов, завоевывают все более сильные позиции на внутреннем рынке страны, осуществляют противозаконные преступные финансовые операции. Такие финансовые операции с использованием криптовалюты проводятся анонимно, без централизованного контроля, что мотивирует преступников к выбору названного средства оплаты для совершения различных преступлений, таких как незаконный оборот наркотических средств и психотропных веществ, незаконный оборот оружия, боеприпасов и взрывчатых веществ, финансирование терроризма и экстремизма, других преступлений в сфере экономической деятельности[13].

---

[12] *Декомпиляция* – процесс, противоположный *компиляции* – способу сборки программы, включающему трансляцию всех ее модулей, написанных на одном или нескольких языках программирования, в эквивалентные программные модули на языке, близком машинному коду.

[13] Президент В. В. Путин 7 июня 2018 г. во время прямой линии по вопросу использования цифровых технологий в финансовой сфере и внедрения инновационных финансовых инструментов констатировал риск их применения, отметил, что «криптовалюты создают возможность отмывания капиталов, ухода от налогов, финансирования терроризма и распространения мошеннических схем». В то же время он подчеркнул, что «необходимо отталкиваться от международного опыта и создавать юрисдикцию, которая сможет координировать взаимоотношения криптовалютности с государственной сферой» [Прямая линия с Владимиром Путиным // Президент России: [сайт]. URL: http://www.kremlin.ru/events/president/news/57692 (дата обращения: 18.05.2018)].

Так, при майнинге[14] могут совершаться преступления, предусмотренные ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ».

Совершение преступления, связанного с использованием криптовалюты, можно рассмотреть на примере материалов следующего уголовного дела.

> В ноябре 2016 г. у гражданина К. возник преступный умысел и корыстная цель, направленные на получение имущественной выгоды, исчисляемой денежными средствами.
>
> Он получил несанкционированный удаленный доступ к электронно-вычислительным машинам других пользователей при помощи вредоносных компьютерных программ, предназначенных для уничтожения, блокирования, модификации, копирования компьютерной информации и нейтрализации средств ее защиты, и использовал вычислительные мощности этих машин для майнинга и конвертации получаемых электронных условных единиц [10].

В последние годы *широкое распространение получили криминальные схемы, связанные с вовлечением офшорных финансовых компаний с использованием в целях легализации денежных средств сети Интернет, кредитных карт, небанковских «альтернативных» систем перевода денежных средств и возможностей международной торговли товарами и услугами*.

Также следует отметить, что достижения компьютерной техники широко применяются при совершении иных преступлений.

> Так, подсудимый Б. пояснил, что от неустановленного лица он получил текстовое сообщение на телефон с предложением забрать «закладку» наркотических средств в размере 16 кг и координатами с фотографией. Наркотики он должен был достать и увезти в хранилище, где разделить на более мелкие партии и разложить по тайникам. Ранее он уже занимался аналогичной деятельностью. За это он должен был получить от неустановленного лица 500 000 рублей посредством перевода средств в криптовалюте биткоин [9].

Данные факты, а также возможность бесконтрольного перевода денежных средств и их последующего обналичивания создают риск потенциального вовлечения криптовалюты в схемы, направленные на легализацию доходов, полученных преступным путем, и на финансирование терроризма, что влечет за собой нарушение прав и законных интересов неопределенного круга лиц, получающих доступ к компьютерной информации. При таких обстоятельствах криптовалюта, в том числе и биткойн, становится «денежным суррогатом», способствует росту теневой экономики Российской Федерации, а введение на территории Российской Федерации других денежных единиц и выпуск денежных суррогатов, согласно законодательству, запрещаются [4, ст. 27].

При рассмотрении и классификации способов совершения преступлений в сфере информационных технологий **помимо перечисленных критериев следует учитывать и такой, как распространенность**.

---

[14] *Майнинг* – вычислительные операции специального характера, позволяющие получить криптовалюту (биткойны), конвертируемую в денежные средства.

Особое место среди преступлений в сфере информационных технологий занимает такой вид распространенных противоправных деяний, как **мошенничество в сфере компьютерной информации**, на характеристике и способах которого мы остановимся подробнее.

Р. С. Белкин еще в начале 2000-х утверждал, что традиционные способы мошенничества в современных условиях уступили место гораздо более опасным видам, причиняющим неизмеримо более значительный ущерб потерпевшим. Это различные виды банковских мошенничеств, изощренные способы использования подложных документов и т. п.

Определяющим криминалистическим признаком мошенничества служит способ его совершения, который, в конечном счете, сводится к обману или злоупотреблению доверием обманутого лица или организации» [14, с. 153].

Анализ научных публикаций о мошенничестве в сфере компьютерной информации приводит нас к выводу о том, что отсутствует единый подход к классификации его способов.

Возможно, это связано со скудным опытом судебной практики расследования такого преступления, ведь в УК РФ рассматриваемая норма была введена относительно недавно, когда в 2012 г. появилась статья 159.6 «*Мошенничество в сфере компьютерной информации*», под которым понимается «хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей» [3, ст. 159.6].

Обратимся к мировой правотворческой практике, а конкретно к ст. 8 Конвенции ООН, регламентирующей преступность в сфере компьютерной информации [1], где выделяются некоторые способы неправомерного лишения лица собственности путем: любого ввода, изменения, удаления или блокирования компьютерных данных; любого вмешательства в функционирование компьютерной системы с мошенническим намерением неправомерного извлечения экономической выгоды для себя или для иного лица [1, ст. 8].

В результате анализа следственной и судебной практики можно выделить *самые распространенные способы совершения мошенничества в сфере компьютерной информации* на территории нашего государства:

1) незаконное завладение регистрационными сведениями из разных учетных записей с последующим их применением, в ряде случаев с использованием в мошеннических схемах;

2) использование платежных сервисов разных интернет-ресурсов во время осуществления иным лицом платежных операций для последующего обналичивания чужих денежных средств или приобретения товаров безналичным путем за счет средств жертвы;

3) размещение ложных сведений для введения в заблуждение на специально созданном сайте о возможностях получения крупной прибыли от краткосрочных вкладов с последующим заключением виртуальных сделок и переводом денежных средств на счет иностранного банка;

4) взлом электронного кошелька с целью хищения денежных средств путем их обналичивания, перевода на другие счета, оплаты услуг либо товаров через электронные платежные системы типа Qiwi, PayPal, «Яндекс Деньги», WebMoney;

5) рассылка на электронную почту спама с вложениями, содержащими вредоносные программы, или со ссылкой, вставленной в сообщение;

6) рассылка писем-«оферт» об инвестировании бизнеса путем пополнения счета. В случае согласия требуется предоставить персональные данные (для юридического лица – образцы подписей, банковские реквизиты и др.);

7) проведение интернет-аукционов и электронных торгов с заведомо несуществующими лотами, где для завышения цены товара мошенники сами делают ставки;

8) создание сайтов-двойников известных интернет-магазинов с целью продажи несуществующих товаров;

9) проведение «благотворительных» акций в Интернете, предлагающих перечислять деньги на счета якобы нуждающихся лиц (тяжело больных, инвалидов и т. п) либо их родственников. Также могут создаваться сайты-двойники реальных благотворительных организаций;

10) хищение номеров платежных карт посредством специального программного обеспечения или с сайтов-двойников, а также путем физического завладения мобильным телефоном, где подключена услуга «Мобильный банк» [68, с. 140].

> Так, Ивановским районным судом Амурской области в 2017 г. был вынесен обвинительный приговор в отношении П., который, завладев сотовым телефоном потерпевшего с установленной в нем сим-картой с подключенной услугой «Мобильный банк», из СМС-сообщения узнал о доступном лимите денежных средств, находящихся на расчетном счете банковской карты ПАО «Сбербанк России», перечислил их себе и использовал в личных целях [7].

Отметим, что перечень открыт и не является исчерпывающим, выше указаны лишь самые распространенные способы мошенничества. По мнению С. А. Потапова, которое мы разделяем, многообразие способов подготовки, совершения и сокрытия преступлений, ведет к увеличению уровня латентности мошенничества в сфере компьютерной информации, а следовательно, затрудняет расследование [76, с. 91].

Способы совершения мошенничества в сети Интернет коррелируют с видами данного преступления, их можно сгруппировать следующим образом:

1) мошенничество в Интернете, совершаемое с использованием средств обмена электронными сообщениями (по электронной почте, через социальные сети, с помощью программ-мессенджеров);

2) мошенничество в Интернете посредством использования специально созданных интернет-сайтов.

Рассмотрим *первую группу – мошенничество в Интернете, совершаемое с использованием средств обмена электронными сообщениями (по электронной почте, через социальные сети, с помощью программ-мессенджеров)*.

Рассылаемые сообщения можно условно разделить на два вида:

– сообщения с целью сбора личных данных о потенциальных жертвах преступления;

– сообщения, в которых имеется предложение совершить денежный перевод на банковскую карту либо сообщить данные банковской карты.

В первом случае вне зависимости от того, какие средства применяются для обмена электронными сообщениями, суть мошеннических действий заключается в массовой рассылке заранее подготовленного спама. Мошенники используют специальные программы – «троянские вирусы», которые собирают личные сведения о потенциальной жертве преступления, как правило, сохранившиеся в истории интернет-браузера. К таким сведениям относятся данные о личности жертвы (паспортные данные, номер социального страхования и т. д.), пароли от электронной почты и иных интернет-ресурсов, а также платежные данные банковской карты. Также мошенники могут рассылать обычные анкеты, при заполнении которых потенциальным жертвам предлагается ввести свои личные данные (такой способ мошенничества в Интернете встречается все реже).

Во втором случае, как правило, рассылаются электронные сообщения якобы от лиц, знакомых потенциальной жертве. Наиболее распространено направление сообщений через аккаунты социальных сетей «Одноклассники», «ВКонтакте» и Facebook. Преступник предварительно взламывает аккаунт определенного лица, после чего рассылает сообщения друзьям, указанным в соответствующем разделе страницы пользователя в социальной сети. Например, это может быть сообщение с просьбой сохранить деньги у себя на карте, чтобы «друг» их не растратил. После этого преступник просит сообщить номер, указанный на лицевой стороне банковской карты. Если потенциальная жертва сообщает данный номер, то вместо денег на номер телефона, привязанный к банковской карте, приходит СМС-сообщение с паролем. Именно указанный пароль пытаются узнать злоумышленники для того, чтобы получить доступ к банковской карте.

Для *второй группы – совершения мошенничества в Интернете при помощи сайтов* – характерны следующие преступные схемы:

– инвестиционная схема;

– предложение заработка;

– схема «Волшебный кошелек»;

– организация псевдоаукционов и недобросовестной интернет-торговли (онлайн-торговли);

– кардинг[15];

– организация онлайн-казино и псевдолотерей;

– клонирование известных сайтов.

Наиболее распространенной разновидностью такого мошенничества является недобросовестная онлайн-торговля.

Чаще всего мошенники продают в Интернете товар, которого нет в наличии, и после получения денег, естественно, не передают его покупателю.

[15] См. значение термина в сноске 4.

Кроме того, нами был выявлен специфический вид мошенничества в Интернете при помощи сайтов и онлайн-торговли, ранее не описанный другими авторами: списание денег с банковской карты пользователя, «повредившего продукцию» интернет-магазина, например якобы разбившего бутылки на интерактивном сайте. Это происходит, когда потерпевший совершает 3D-прогулку по нарисованному торговому залу и после движения курсором мышки, по утверждению «владельца онлайн-магазина», «разбивает» виртуальный товар. После этого назначается штраф, который списывается с банковской карты, данные которой потенциальный покупатель сообщил при регистрации на сайте магазина.

Способы сокрытия преступлений в сфере информационных технологий (компьютерной информации) в большей степени коррелируют со способами их совершения.

Например, *способы программного сокрытия следов в Интернете* также многообразны, как и способы совершения преступлений в нем. В целях уничтожении, маскировки и фальсификации следов преступной деятельности преступники могут:

1) использовать ремейлеры[16];

2) создавать вымышленный адрес отправителя письма по электронной почте;

3) работать с программами специального назначения, например такими, как онлайн-анонимайзеры[17]. Поскольку популярность анонимного серфинга[18] в Интернете резко возросла, Tor, VPN, другие сервисы позволяют обезопасить конфиденциальную информацию и получить доступ к сайтам и сервисам, по разным причинам недоступным при обычном подключении. Получается, что анонимайзер – это программное средство, позволяющее злоумышленнику скрыть идентифицирующую информацию о своем компьютере, сменить IP-адрес, сделать невозможным установление личности по трафику при совершении преступлений в сфере информационных технологий;

4) использовать второй электронный почтовый ящик, откуда рассылать интернет-контент, содержащий вредоносный код.

Способы сокрытия преступлений в сфере компьютерной информации *зависят от степени квалификации преступника, его знаний и опыта работы со средствами электронно-вычислительной техники*.

При непосредственном доступе к компьютерной информации и средствам ее обработки сокрытие следов преступной деятельности ограничивается

---

[16] *Ремейлер* (транскрипция англ. *remailer* – «отправитель, переадресатор») – это сервер, получающий сообщение электронной почты и переправляющий его по адресу, указанному отправителем. В процессе переадресации вся информация об отправителе уничтожается, поэтому конечный получатель лишен возможности выяснить, кто является автором сообщения. Некоторые из ремейлеров позволяют также шифровать письма и указывать фиктивный адрес отправителя, но большинство из них прямо сообщают в заголовке, что электронное сообщение анонимно. В качестве ремейлеров могут выступать специализированные веб-сайты, открытые SMTP-серверы и анонимная сеть Mixminion.

[17] *Анонимайзер* – общее название средств для скрытия информации о компьютере, его IP-адресе или пользователе в сети от удаленного сервера.

[18] *Серфинг* – перемещение по различным сайтам.

воссозданием обстановки, предшествующей совершению преступлений, то есть уничтожению оставленных следов (следов рук, микрообъектов и т. д.).

При опосредованном (удаленном) доступе сокрытие заключается в самом способе совершения преступления, который затрудняет обнаружение неправомерного доступа, распространения вредоносных программ. Это достигается использованием чужих паролей, идентификационных и биометрических средств доступа и др. [24, с. 35].

Таким образом, можно констатировать, что способ совершения преступления среди данных, составляющих криминалистическую характеристику, являются особо значимым, так как имеет разветвленные корреляционные связи, позволяющие определить комплекс других обстоятельств противоправного деяния.

Существует прямая зависимость количества (множественности) способов совершения преступлений в сфере информационных технологий от совершенствования этих самых технологий. Их развитие происходит параллельно, в связи с чем не представляется возможным составить закрытый перечень способов.

§ 3. Специфика механизма следообразования при совершении преступлений в сфере информационных технологий

Способы совершения отдельного преступления в сфере информационных технологий определяют специфику механизма следообразования.

Под *механизмом следообразования* понимается «специфическая конкретная форма протекания процесса, конечная фаза которого представляет собой образование следа-отражения» [15, с. 118].

Элементами механизма являются *объекты следообразования:* следообразующий, следовоспринимающий и вещество следа.

Следы совершения преступления в сфере информационных технологий нечасто остаются в виде изменений внешней среды. В основном они не рассматриваются современной трасологией, так как обычно носят информационный характер, то есть являются изменением в компьютерной информации, представляя форму ее модификации, копирования, уничтожения, блокирования.

Электронная информация, как правило, обезличена и не содержит однозначных данных о ее авторстве, так как не оставляет о себе подобных данных. Тем не менее, файл с электронной информацией в большинстве случаев содержит метаданные, в которых может быть указан, помимо даты создания, изменения, и автор документа, однако эти данные невозможно доподлинно проверить.

В криминалистическом учении традиционно **принято делить следы на две основные группы**: *материальные*, то есть зафиксированные путем изменения внешней среды, и *идеальные* – оставшиеся в памяти людей (потерпевшего, преступника, свидетелей). Однако П. В. Мочагин предлагает к двум традиционным формам следообразования добавить еще одну – в виртуально-информационной и технико-компьютерной сфере [70, с. 98]. Такие следы предложено именовать *виртуальными*. В. А. Мещеряков трактует их как любое изменение состояния автоматизированной информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации [35, с. 25].

Данная позиция является неоднозначной, так как другие авторы не выделяют следы в сфере компьютерной информации в отдельную группу, аргументируя свою позицию тем, что это будет способствовать загромождению разработанных криминалистикой положений о рассматриваемых проблемах [63, с. 287]. Они считают, что такие следы нужно идентифицировать в качестве материальных, но представляющих особую форму, – следов-отображений, зафиксированных на электронных цифровых носителях [56, с. 3]. А. Б. Коновалова вслед за другими авторами предлагает терминологически обозначить такую категорию следов как «бинарные следы», отображающие результаты действий с двоичным кодом электронно-вычислительной машины [65, с. 113].

Вопрос остается достаточно спорным, так как специфика образования, обработки и хранения компьютерной информации предусматривает использование компьютерно-технических средств, которые являются материальными. Таким образом, на носителях указанных средств возможно материально фиксированное отображение компьютерной информации. Поэтому в качестве следов преступлений в сфере компьютерной информации можно рассматривать электронные сигналы или команды, отправленные преступником со своего компьютера. Эти сигналы имеют также материально фиксированное выражение (IP-адрес, MAC-адрес – см. подробнее об этих понятиях ниже), что позволяет их с большой точностью идентифицировать.

Однако, дефиниция «виртуальные следы» уже вошла в обиход наряду с материальными и идеальными следами. Так, согласно проведенному О. Ю. Введенской исследованию, преступность в сфере компьютерной информации оставляет за собой: виртуальные следы в виде кэш-файлов, IP-адресов, журналов историй и т. п. – по мнению 27 % опрошенных представителей правоохранительных структур; материальные следы – по мнению 24 %; идеальные следы в виде показаний потерпевших, свидетелей, подозреваемых (обвиняемых) – по мнению 22 % [52, с. 210].

Принимая во внимание вышеизложенное, **целесообразно следы преступлений, совершаемых в сфере информационных технологий, разделить на два типа**: традиционные следы (материальные, идеальные) и нетрадиционные – компьютерно-технические.

К *традиционным материальным следам* можно отнести следы на самой вычислительной технике: следы пальцев рук, микрочастицы на клавиатуре, иных составных частях компьютера.

Традиционные идеальные следы представляют собой запечатление события преступления и элементов механизма его совершения в памяти и сознании. Такие следы обусловлены психофизиологическими процессами организма человека и имеют вид мысленных образов о совершенном преступлении или его фрагментах [15, с. 199].

Термин *«компьютерно-технические следы»* в лексиконе криминалистики появился сравнительно недавно [78, с. 43], а ведь появление новых объектов, средств и способов совершения преступлений в сфере информационных технологий требует своевременной реакции со стороны ученых-криминалистов.

Указанные следы остаются прежде всего на компьютерно-технических носителях информации, отражая, при сравнении с исходным состоянием, изменение хранящейся в них информации. Речь идет о модификации информации, находящейся в базах данных, программах, файлах, учетных записях в сети Интернет и т. п., на флеш-картах и жестких дисках компьютеров. К компьютерно-техническим следам относят также результаты работы антивирусных программ, которые возможно выявить путем изучения компьютерного оборудования, протоколов работы программ, рабочих записей программистов и др.

Помимо распространенных мест поиска следов преступления, которыми являются место нахождения преступника и место происшествия, следы преступлений в виде компьютерной информации могут быть обнаружены при передаче по каналам связи либо в месте хранения и автоматизированной обработки с использованием вычислительных мощностей, то есть **к месту поиска следов и источникам криминалистически значимой информации относятся**:

– рабочее место преступника (компьютерные устройства, электронные носители информации, средства связи, записи);

– место происшествия (компьютерная система);

– сетевые ресурсы преступника (в локальной сети и глобальной сети);

– каналы связи преступника (сетевой трафик);

– легальные сетевые ресурсы, используемые в преступной деятельности (почтовые серверы, вычислительные мощности провайдеров хостинга, ресурсы провайдера по предоставлению доступа в Интернет и т. п.). Яркой особенностью подобных следов является то, что для их выявления необходимо привлечение специалиста.

В случае выявления сетевых ресурсов в Интернете, используемых для осуществления преступной деятельности, источниками криминалистически значимой информации являются:

1) данные провайдеров хостинговых услуг:

– журнальные файлы (лог-файлы) подключений к арендуемому сетевому ресурсу;

– цифровые копии содержимого серверов или облачных хранилищ информации.

Изучение лог-файлов подключений к серверу, использующемуся в криминальной деятельности, позволяет обнаружить сетевые адреса пользователей этого ресурса и принять меры к установлению их личности. Если реальный IP-адрес пользователя скрыт прокси-сервером, необходимо, при наличии возможности, повторить операцию по поиску адресов и попытаться проследовать по их цепочке.

В ходе исследования копий содержимого серверов могут быть подтверждены факты их использования при совершении киберпреступлений, обнаружены экземпляры распространяемых вредоносных программ, выявлены сетевые реквизиты пользователей – имена учетных записей и IP-адреса подключений, а также адреса других серверов сетевой инфраструктуры;

2) данные провайдеров доступа в сеть Интернет:

– журнальные файлы доступа в Интернет;

– статистические данные учета сетевого трафика.

Лог-файлы и статистические данные учета сетевого трафика, собираемые интернет-провайдером, содержат сведения о сетевой активности пользователей конечных устройств, которыми могут быть как преступники, так и потерпевшие. В любом случае информация может представлять интерес для следствия и использоваться для выявления сетевых адресов, с которыми конечные устройства взаимодействовали (серверы управления и распространения вредоносных программ, форумы криминальной направленности, виртуальные обменные и платежные сервисы и т. п.) [78, с. 44].

Если конкретизировать традиционную классификацию электронно-цифровых следов, то при выявлении преступлений в сфере информационных технологий *основной объем необходимых действий правоохранительных органов сводится* к установлению сведений от оператора связи, оказывающего телематические услуги, а также выяснению конкретного пользователя путем соотнесения полученных сведений.

Указанную **информацию об электронно-цифровых следах можно получить путем исследования**:

1) регистрационных данных по IP-адресу, с которого были осуществлены преступные действия;

2) сведений об отправителе электронного письма;

3) сведений о владельце электронного почтового ящика;

4) данных средств вычислительной техники по MAC-адресу [34, с. 25].

Первый путь – исследование регистрационных данных по IP-адресу.

IP-адрес – это набор из четырех десятичных чисел, разделенных точками, универсальный идентификатор средства компьютерной техники в Интернете. По функциям IP-адрес можно сравнить с почтовым адресом.

Различают статические и динамические IP-адреса. Статический – постоянный адрес, который каждый раз присваивается определенному пользователю – владельцу адреса, он обеспечивает повышенную надежность авторизации. Динамический IP-адрес присваивается каждому подключаемому к Интернету сетевому устройству, если ему не присвоен статический IP-адрес.

Мобильные операторы присваивают IP-адрес по абонентскому номеру. Каждому оператору связи Роскомнадзор определяет свой диапазон IP-адресов.

Для определения принадлежности IP-адреса конкретному оператору можно:

1) воспользоваться глобальным справочным интернет-сервисом Whois (например, по адресам: https://whois.ru/; https://speed-tester.info), предоставляющим информацию о регистрационных данных владельцев IP-адресов и доменных имен. На открывшейся странице нужно выполнить ряд действий: заполнить графу «Введите домен или IP» или перейти по ссылке «Узнать чужой IP» и заполнить нужные поля на новой вкладке и др. Так, на сайте «speed-tester.info» сервис определения чужого IP-адреса находится на вкладке https://speed-tester.info/check_another_ip.php. В итоге появятся сведения об операторе связи, стране, городе и др.;

2) направить запрос установленному оператору о предоставлении регистрационных данных абонента.

Пример запроса регистрационных данных IP-адреса:

…прошу предоставить регистрационные данные абонента, которому был выделен IP-адрес… *(например, 87.23.123.32)* в следующие периоды времени… *(указываются точные дата и время)*.

Второй путь – исследование сведений об отправителе электронного письма.

IP-адрес может быть определен по данным электронного письма, которое содержит информацию о маршруте следования в процессе отправки-получения. Анализ такой информации позволяет получить сведения об IP-адресе электронно-вычислительной машины, с которого оно было отправлено, и реальном электронном почтовом ящике, так как в ряде случаев при получении письма в поле «От кого» может быть указан произвольный электронный почтовый ящик, в том числе не принадлежащий подозреваемому.

Как правило, по умолчанию информация о движении электронного письма получателю не отображается. В зависимости от используемого почтового клиента можно ознакомиться со свойствами письма, выбрав на командной панели определенный заголовок, например «Служебные заголовки».

Название строки в меню (она, в свою очередь, может скрываться за знаком «…» или надписью «Еще») для некоторых популярных почтовых клиентов, используемых в Российской Федерации:

– «Служебные заголовки» – mail.ru;
– «Свойство письма» – yandex.ru;
– «Показать оригинал» – gmail.com;
– «Показать исходник» – mozilla.

Процесс получения регистрационных данных и информации о соединениях по установленному IP-адресу описан выше.

В целях *установления владельца электронного почтового ящика* (*третий путь*) необходимо прежде всего:

1) исследовать название: yyy@xxx.ru, где yyy – имя пользователя (логин), xxx – адрес сервиса электронной почты (например, mail.ru);

2) выяснить принадлежность электронного почтового ящика конкретному сервису электронной почты.

Наиболее популярные сервисы электронной почты

E-mail	Компания	Юридический адрес
@mail.ru @inbox.ru @bk.ru @list.ru	ООО «МЭЙЛ.РУ ГРУП»	125167, Россия, Москва, Ленинградский проспект 39, стр. 79
@yandex.ru	ООО «Яндекс»	119021, Россия, Москва, ул. Льва Толстого, 16
@rambler.ru @lenta.ru	ООО «Рамблер Интернет Холдинг»	115280, Россия, Москва, Ленинградская слобода, д. 26, стр. 1

Сведения о регистрации и администрировании почтовых ящиков @gmail.com, @google.com, @yahoo.com (и прочие) находятся на оборудовании организаций, осуществляющих деятельность за пределами Российской Федерации. Получить их возможно только посредством направления запроса о правовой помощи при взаимодействии с Национальным центральным бюро МВД России в регионе, например с НЦБ Интерпола Управления МВД России по Хабаровскому краю;

3) направить запрос о предоставлении регистрационных данных и активности электронного почтового ящика.

Пример запроса регистрационных данных владельца электронного почтового ящика:

…прошу предоставить регистрационные данные IP-адреса авторизации, абонентский номер активации и восстановления пароля владельца электронного почтового ящика…

В полученном ответе будет информация об IP-адресах, с которых владелец управлял электронным почтовым ящиком;

4) направить необходимые запросы для получения информации по IP-адресу.

Четвертый путь – установление средств вычислительной техники по MAC-адресу.

У каждой сетевой карты в электронно-вычислительной машине: на ноутбуке, в планшетном компьютере, смартфоне – имеется уникальный идентификационный номер (MAC-адрес, физический адрес), который присваивается производителем на заводе. Он имеет примерно следующий вид: 00-04-5F-D4-CF-B6.

С целью розыска компьютерной техники и лица, которое предположительно совершило преступление, необходимо:

1) выяснить MAC-адрес похищенного компьютера. Необходимые сведения уточняются по документам, чекам на приобретенный товар либо направляется запрос интернет-провайдеру, который подключал компьютер;

Пример запроса:

…прошу предоставить MAC-адрес сетевого оборудования абонента Иванова А. А., подключенного по адресу…

2) направить запросы операторам связи страны, если имеются подозрения что электронно-вычислительная машина использовалась на территории Российской Федерации, чтобы установить факт активации оборудования в их сетях.

Пример запроса:

…прошу сообщить, регистрировалось ли сетевое оборудование с MAC-адресом 00-04-5F-D4-CF-B6 в ваших сетях.

Если да, то прошу предоставить сведения о лице, с которым заключен договор на предоставление услуг связи, а также адрес установки оконченного оборудования…

MAC-адрес сетевого адаптера электронно-вычислительной машины передается оператору связи только при непосредственном подключении компьютера к его оборудованию. Если для подключения электронно-вычислительной машины используется промежуточное оборудование (например, ADSL-модем,

Wi-Fi-маршрутизатор, USB-модем), то MAC-адрес компьютерной техники оператору не передается. Кроме того, значение MAC-адреса может принудительно изменяться на произвольное число самим пользователем, что предусмотрено настройкой соответствующих параметров в операционной системе.

Если на похищенном компьютере при включении автоматически при открытии браузера запускается почтовый ящик потерпевшего либо сохранены в настройках веб-обозревателя пароли от социальных сетей, то необходимо сделать соответствующие запросы для сбора информации об электронном почтовом ящике, персональной странице, электронном кошельке, а затем – сведений по полученным IP-адресам. При этом необходимо запретить владельцу самому посещать страницы в соцсетях, пользоваться электронными почтой, кошельком и т. п. до получения ответов [34, с. 12].

Большое значение имеет безотлагательность данных мероприятий, что обусловлено свойствами компьютерной информации. Целесообразно их провести на этапе выявления факта интернет-преступления в рамках оперативно-разыскной деятельности, а также в рамках поисковых мероприятий, оперативного сопровождения предварительного расследования.

Что касается **вопроса выяснения конкретного пользователя**, то с *идентификацией пользователя мобильного Интернета вопрос не очень сложен*. Поскольку IP-адрес привязан к номеру мобильного телефона, который зарегистрирован на конкретного пользователя, то действия должны быть направлены на отработку причастности к совершенному преступлению владельца симкарты, а также на установление лиц, имеющих возможность ей воспользоваться.

С идентификацией же пользователей Интернета в иной форме вопрос гораздо сложнее. Даже установление владельца IP-адреса не позволит сделать вывод о его виновности. В настоящее время нет ни одного эффективного способа идентификации конкретного пользователя Интернета. Необходимо отметить, что работа для нахождения такого способа проводится как на законодательном, так и на организационном уровне путем внесения всевозможных предложений. Однако сложившаяся ситуация показывает, что она малоэффективна. Сегодня установление личности интернет-преступника возможно лишь с помощью грамотного и безотлагательного проведения оперативно-разыскных мероприятий и следственных действий [16, с. 22].

Подведем итог. Рассматривая позицию об акценте на информационной сущности материальных следов, необходимо заметить, что нельзя преуменьшать роль традиционных криминалистических (трасологических) следов, ведь они также несут в себе информацию о совершенном деянии.

Тем не менее, совершение преступлений в сфере информационных технологий способствует выделению отдельной группы следов, отличных по своим признакам от традиционных материальных и идеальных. Можно заключить, что виртуальные следы занимают промежуточное положение между материальными и идеальными, представляют собой отдельную группу следов, которые должна рассматривать криминалистика.

Вопросы для самостоятельного изучения

1. Общая характеристика преступлений, совершаемых в сфере информационных технологий.
2. Научные, правовые и организационные основы расследования преступлений в сфере информационных технологий.
3. Криминалистическая характеристика преступлений в сфере информационных технологий.
4. Способы подготовки, совершения и сокрытия преступлений в сфере информационных технологий.
5. Сопутствующие преступления, совершаемые с использованием компьютерной техники, их виды и способы совершения.
6. Типичные следы преступлений в сфере информационных технологий и их классификация.
7. Механизм образования и локализации электронно-цифровых следов при совершении преступлений в сфере информационных технологий.
8. Характеристика следообразующих и следовоспринимающих объектов при совершении преступлений в сфере информационных технологий и способы их изъятия.

ГЛАВА 2. ОСОБЕННОСТИ ВОЗБУЖДЕНИЯ УГОЛОВНЫХ ДЕЛ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Типичные следственные ситуации и версии, складывающиеся на первоначальном этапе расследования преступлений в сфере информационных технологий

На первоначальном этапе расследования преступлений в сфере информационных технологий (компьютерной информации) следователь действует в условиях недостаточности исходных данных по делу. Имеющиеся признаки преступления, как правило, могут быть истолкованы неоднозначно. При этом большинство следов являются электронно-цифровыми, поэтому не персонифицируют преступника. В таких условиях находит применение положение, высказанное В. Е. Корноуховым: «…для решения той или иной задачи должны разрабатываться и отражаться в методике несколько комплексов следственных действий и оперативно-розыскных[19] мероприятий, которые были бы адаптивны к разным условиям расследования преступлений» [66, с. 172]. Близкой точки зрения придерживается А. С. Шаталов, который обращает внимание на важность выработки алгоритмов расследования преступлений. Он пишет, что следователь постоянно сталкивается с проблемой, какие проводить следственные действия, в какой очередности, с чьим участием и т. д. Существующие или выработанные следователем путем апробации, *алгоритмы и программы расследования должны быть максимально индивидуализированы, рассмотрены с точки зрения конкретной следственной ситуации*. В противном случае применение одной и той же программы, алгоритма действий может привести к достижению противоположных результатов, вплоть до появления следственных ошибок [43, с. 25].

Ситуационный подход эффективно упорядочивает действия следователя, поэтому в современной криминалистической науке он занимает одно из центральных мест. Благодаря его использованию следователь экономит силы и время, затрачиваемые на поиск решения следственных ситуаций, имеющих, в сущности, типовое содержание и неоднократно попадающихся в практике. Полагаем, правильно считать, что *следственная ситуация* – это та обстановка, которая создается при расследовании преступления и объективно отражает внутреннее состояние, ход и условия расследования на основе совокупности фактических и иных данных.

Общими для любой следственной ситуации элементами являются следственные и оперативно-разыскные[19] данные о способе и механизме

[19] Различия в написании одного и того же слова обусловлены следующим. *Слова с частью «разыск-» с безударным «а» в приставке* (разыскной, оперативно-разыскной) пишутся в учебном пособии через «а» в соответствии с правилами орфографии современного русского языка. Не соответствующее сегодняшним нормам написание через «о» сохранено в официальном названии закона «Об оперативно-розыскной деятельности» как традиционное на момент его принятия, в прямых цитатах из этого документа и из научных, учебных и других изданий, а также в их названиях в списке использованных источников. – *Прим. ред.*

преступления, личности преступника, обстановке, цели и мотиве преступного посягательства, данные об обстановке, в которой проводится расследование, сведения о факторах, затрудняющих следственные действия и препятствующих им, и т. д. Роль и значение следственных ситуаций определяются тем, что они выступают в качестве основы для построения *версий,* то есть «обоснованных фактическими данными предположений следователя, вероятностно устанавливающих еще не доказанные обстоятельства и одновременно правдоподобно объясняющих выявленную исходную информацию» [44, с. 18].

Базовым компонентом следственных ситуаций является *типичная следственная ситуация*, которая требует своих тактико-технических приемов для разрешения. Она обладает устойчивым комплексом признаков, включающих в себя «общие черты хода и состояния расследования к определенному его моменту» [33, с. 21], отражающих сущностные черты криминалистической характеристики данного вида преступлений и наиболее вероятную обстановку их расследования. *Типичная ситуация отличается от конкретной*, формирующейся при расследовании определенного дела и характеризующейся частными индивидуальными особенностями обстановки и связями, возникающими при его расследовании [21, с. 309].

На основе совокупности криминалистически значимых данных, характерных для соответствующих ситуаций, можно выдвигать **типичные следственные версии**:

1) заявление о преступлении в сфере компьютерной информации подтверждается, преступление действительно имеет место;

2) заявитель ошибается или заблуждается: преступления в сфере компьютерной информации не было, а совершено другое преступление;

3) имеет место ложное заявление о преступлении в сфере компьютерной информации.

Отметим, что в литературе выделяются и другие следственные версии, например: «совершено иное преступление, сбой компьютерного оборудования применен для запутывания следов преступления» [71, с. 49]. Представляется, что это более сложная следственная ситуация, в которой преступление в сфере компьютерной информации все равно имело место (в виде «сбоя компьютерного оборудования»), но наряду с другим преступлением.

Что касается **преступлений в сфере компьютерной информации,** оригинальной представляется **классификация типичных следственных ситуаций**, предлагаемая Н. Н. Ахтырской, полагающей, что эти ситуации существенным образом зависят от обстоятельств, подлежащих установлению и доказыванию по уголовному делу. В соответствии с этим автор выделяет четыре группы следственных ситуаций. В первой объединены преступления, предметом которых являются средства компьютерной техники; во второй – преступления, где эти средства выступают в качестве предмета и средства совершения преступления одновременно; в третьей – где компьютерные средства служат для совершения и сокрытия преступлений; в четвертой – те в которых средства компьютерной техники «выступают источником криминалистически значимой информации» [46, с. 133].

Более значимым в практическом плане представляется деление следственных ситуаций на следующие группы:

1) *конфликтные ситуации*, при которых субъект преступления обладает информацией, но умышленно искажает или скрывает ее;

2) *бесконфликтные ситуации*, при которых субъект преступления объективно передает следователю искомую информацию, не стремится ее искажать или утаивать;

3) *слабоконфликтные ситуации*, которые возникают в ситуациях допроса, когда допрашиваемый обладает искомой информацией, желает ее передать, но в силу субъективных или объективных факторов воспринял, запомнил и, соответственно, передает ее с искажениями.

При расследовании дел о преступлениях в сфере компьютерной информации интерес представляет распространенная типичная ситуация, характеризующаяся возникновением конфликта между следователем и потерпевшим, которую можно назвать «*парадоксальной конфликтной*». В этой ситуации сами потерпевшие оказывают пассивное или активное сопротивление следствию, стремясь скрыть имевшие место обстоятельства преступления, например, пытаясь таким образом защитить репутацию своей организации, не сумевшей сохранить конфиденциальную информацию; опасаясь наказания за свою халатность и т. п. [74, с. 21]. Согласно данным анкетирования, проведенного В. В. Поляковым среди следователей одного из управлений внутренних дел и сотрудников управления Федеральной службы безопасности, такая ситуация при проведении следственных действий встречались в 12 % случаев [75, с. 47].

Особую роль для построения эффективной методики предварительного расследования играет **выделение следственных этапов, объединяющих проверочные и следственные действия в соответствии с имеющей место следственной ситуацией**.

Можно выделить этап предварительной проверки полученных сведений о преступлении, а также первоначальный (неотложный), последующий и заключительный этапы расследования. Это, на наш взгляд, оправданно, так как упорядочивает криминалистическую систему знаний при разрешении уголовного дела по существу.

С позиций ситуационного подхода *первоначальный этап расследования преступлений в сфере компьютерной информации может быть охарактеризован тремя типичными следственными ситуациями*, классифицируемыми по субъекту, выявившему преступление:

1) собственник компьютерной информации обнаружил факт преступления и самостоятельно установил преступника;

2) собственник компьютерной информации обнаружил факт преступления, но преступник остается неустановленным;

3) преступление выявили правоохранительные органы [32, с. 468].

В случае когда идет речь о преступлении в сфере компьютерной информации, эта классификация представляется неполной и должна включать, по нашему мнению, еще одну типичную следственную ситуацию: преступление выявлено иным лицом, в качестве которого обычно выступает организация-

провайдер, обслуживающая собственника конфиденциальной информации. Отметим, что провайдер также может быть потерпевшим.

Типичная доследственная ситуация на предварительном этапе в случае совершения преступления при помощи удаленного доступа к компьютерной информации характеризуется тем, что потерпевшие (физические или юридические лица) сами обнаруживают преступление. Именно они устанавливают факт снятия провайдером со своих счетов определенных сумм за информационные услуги, которые они не получали, обращаются за разъяснением к провайдеру, а затем с заявлением – в следственные органы.

Пограничная с этой ситуация – при которой доступ к средствам компьютерной техники затруднен из-за умышленных действий опытных и квалифицированных преступников. Такие преступники широко применяют последние научно-технические достижения в области шифрования информации. Стремясь скрыть следы противоправной деятельности, они могут устанавливать специальные программно-аппаратные средства для уничтожения и блокирования значимой для следствия информации при обращении к ней посторонних лиц. В то же время современные технические средства защиты компьютерной информации включают в себя широкий арсенал программно-аппаратных эффективных средств криптографической защиты, таких как электронная подпись, электронно-цифровые ключи, свободно продаваемые компьютерными фирмами.

Весьма распространенной ситуацией является заражение криминалистически значимой компьютерной информации вредоносными программами (вирусами). В большинстве случаев это не связано с сокрытием следов преступления или противодействием следствию со стороны преступников.

При производстве следственных действий на данном этапе вызывает сложность *проблемная ситуация*. Она характеризуется отсутствием заранее определенной, однозначной, жесткой программы нахождения информационных и тактических решений. Проблемную ситуацию отличает неполное, недостаточное знание о том, как было совершено преступление в сфере компьютерной информации, кем оно совершено и каким образом. В связи с этим оптимальным способом разрешения такой ситуации являются построение и проверка следственных версий, ориентированных на предмет доказывания. Повышенную сложность при расследовании представляет установление конкретного лица, совершившего преступление, которое, как правило, на первоначальном этапе неизвестно ни следствию, ни потерпевшим. В силу этого «заранее определенная» программа построения адекватных следственных действий отсутствует, следователю приходится выдвигать версии, которые должны исходить из теоретических знаний и обобщения практики. Именно в этих условиях в большей степени проявляется роль ситуационного подхода и изучения типичных следственных ситуаций в частности [36, с. 112].

На последующем этапе расследования у следователя появляется доказательственная база. На этом этапе *типичными ситуациями являются* следующие:

1) признание вины обвиняемым;

2) полное отрицание вины;

3) частичное признание вины.

Складывающаяся ситуация определяет дальнейшее направление расследования вплоть до принятия следователем окончательного решения по делу.

Следственные ситуации на данном этапе расследования дел о преступлениях в сфере инормационных технологий можно охарактеризовать как преимущественно бесконфликтные или слабоконфликтные. Более того, нередко возникает типичная следственная ситуация деятельного раскаяния, открывающая наибольшие возможности для собирания и исследования доказательств по уголовному делу. В частности, при допросах лица, проявившего деятельное раскаяние, может быть получена ценная информация о других преступлениях, об условиях, сделавших данное преступление возможным, что позволит в дальнейшем предупредить совершение подобных преступлений.

Следует отметить, что при получении признательных показаний в отдельных случаях может потребоваться их проверка, так как возможна ситуация, связанная с принятием вины преступника на себя другим лицом (самооговор). Во многом это связано с тем, что большинство следов компьютерного преступления не имеют персонифицирующего характера. Преступник, для того чтобы избежать ответственности, может прибегать к следующим приемам: шантажу и угрозам физическим насилием, подкупу, использованию доброго отношения к себе со стороны близких ему людей и т. д.

Таким образом, изучение приведенных и других ситуаций, возникающих на предварительном следствии, является основанием для выбора и использования нужной группы криминалистических рекомендаций. Знание этих рекомендаций может в значительной степени способствовать эффективному сбору доказательств по преступлениям, связанным с использованием средств компьютерной техники, особенно по преступлениям, совершенным дистанционно.

§ 2. Организация оперативно-разыскных мероприятий, взаимодействие следователя с органами дознания при расследовании преступлений в сфере информационных технологий

Успех расследования преступлений в сфере информационных технологий и проведения предварительной проверки в рамках возбуждения уголовного дела *зависит от четкой организации оперативно-разыскных мероприятий и тесного взаимодействия следственно-оперативной группы с другими подразделениями органов внутренних дел*.

Борьба с преступлениями в сфере высоких технологий *на федеральном уровне* **осуществляется** *Управлением «К» МВД России*.

Основными задачами этого подразделения являются выявление, предупреждение, пресечение и раскрытие:

1) преступлений в сфере компьютерной информации:

– неправомерного доступа к охраняемой законом компьютерной информации;

– создания, использования и распространения вредоносных компьютерных программ;

– нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей;

– мошенничеств в сфере компьютерной информации;

2) преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) и направленных против здоровья несовершеннолетних и общественной нравственности:

– изготовления и распространения материалов или предметов с порнографическими изображениями несовершеннолетних;

– использования несовершеннолетнего в целях изготовления порнографических материалов или предметов.

3) преступлений, связанных с незаконным оборотом специальных технических средств, предназначенных для негласного получения информации.

4) преступлений, связанных с незаконным использованием объектов авторского права или смежных прав [34, с. 3].

На региональном уровне функционируют соответствующие структурные подразделения – *отделы «К»*.

В рамках взаимодействия по уголовному делу, в ходе производства следственных и иных процессуальных действий *могут быть привлечены* также сотрудники оперативно-технических подразделений правоохранительных органов; специалисты по сетевым средствам вычислительной техники; операторы автономных серверов и персональных электронно-вычислительных машин; администраторы сети электронно-вычислительных машин или электросвязи; специалисты обладающие знаниями об операциях технологического процесса, при которых проявились признаки противоправного деяния; операторы, осуществляющие фото- и видеофиксацию следственного действия.

Сотрудникам оперативных подразделений необходимо тщательным образом изучить **стратегию и тактику применения используемых в расследовании рассматриваемых преступлений форм оперативно-разыскной деятельности, а также особые условия проведения оперативно-разыскных мероприятий**.

Под *оперативно-разыскными мероприятиями* мы вслед за С. И. Захарцевым понимаем «составную часть оперативно-розыскной деятельности, сведения об организации и тактике которой составляют государственную тайну, представляющую собой совокупность действий специально уполномоченных на то государственных органов и их должностных лиц, осуществляемых с соблюдением регламентированных законом оснований и условий, отвечающую нормам морали и нравственности и непосредственно направленную на достижение целей и разрешение задач оперативно-розыскной деятельности» [25, с. 92].

Сведения, имеющие значение для раскрытия и расследования преступлений в сфере компьютерной информации, могут дать три основных источника:

– во-первых, сообщения осведомленных лиц об обстоятельствах подготовки и совершения преступлений;

– во-вторых, электронные ссылки на материалы, запрещенные к распространению (в частности, всякого рода базы данных с личными, финансовыми и другими сведениями о населении страны);

– в-третьих, следы противоправной деятельности (например, сайты-двойники, лог-файлы серверов и др.).

Помимо этого, нужные данные можно найти посредством анализа переписки по электронной почте подозреваемых лиц, журналов сервисов обмена сообщениями в режиме реального времени.

Ключевым критерием эффективного осуществления оперативно-разыскных мероприятий в процессе расследования компьютерных преступлений выступает знание и понимание их специфики.

Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» [6] предусмотрены как специальные мероприятия – снятие информации с технических каналов связи и получение компьютерной информации, так и иные мероприятия, в ходе которых может быть произведен поиск, обнаружение и изъятие компьютерных данных.

Система оперативно-разыскных мероприятий осуществляется комплексно и выглядит следующим образом:

– сбор образцов для исследования;

– снятие информации с технических каналов связи;

– получение компьютерной информации;

– исследование;

– прослушивание телефонных переговоров [26, с. 26].

С позиции расследования компьютерных преступлений заслуживает внимания исследование такого оперативно-разыскного мероприятия, как **снятие информации с технических каналов связи**.

На наш взгляд, такое оперативно-разыскное мероприятие является ключевым при расследовании всех преступлений в сфере информационных технологий. Кроме того, снятие информации с технических каналов связи выступает в качестве одного из перспективных с позиции развития техники и тактики применения.

Технические способы связи, в частности через Интернет, давно стали популярными, между тем получают развитие и иные виды технической связи (например, видео-конференц-связь, IP-телефония, радиолокационная связь). Ученые полагают, что впоследствии может иметь место разграничение на законодательном уровне нескольких форм снятия информации с технических каналов связи в зависимости от ее вида [См., например: 42, с. 74]. Мы считаем, что в разделении по такому критерию нет необходимости: классификация различных видов оперативно-разыскных мероприятий по специфике их осуществления согласно ст. 8 Федерального закона «Об оперативно-розыскной деятельности» [6] является максимально эффективной.

Сведения могут находиться в одной из двух форм: статической (хранение на машинном носителе) и динамической (передача по каналу связи). Снятие информации с технических каналов связи производится применительно к сведениям, которые передаются посредством их сбора в реальном времени с помощью

перехвата за счет применения специального оборудования и программного обеспечения.

Специфика этого оперативно-разыскного мероприятия в том, что данные, которые подлежат съему, находятся в электронно-цифровой форме. Полученные данные записываются или копируются на определенные физические носители информации: карты памяти, жесткие диски и др.

Снятие информации с технических каналов связи осуществляется сотрудниками оперативных подразделений правоохранительных органов. Это также могут сделать сотрудники организаций – владельцев технических каналов и соответствующих данных.

Результаты снятия информации фиксируются сотрудником оперативного подразделения *в рапорте или справке*, к которым прилагаются соответствующие носители (помещенные в упаковку и опечатанные) с полученными сведениями, а также, если есть необходимость, распечатки данных сведений [80, с. 82].

В настоящее время широко распространена IP-телефония. Часто данный вид связи комбинируется с обычной и/или мобильной телефонной связью. В такой ситуации следует иметь в виду, что, помимо снятия информации с технических каналов связи, следует также проводить такое оперативно-разыскное мероприятие, как **прослушивание телефонных переговоров**.

Результаты прослушивания переговоров по их целевому использованию можно условно разделить на три категории:

1) результаты прослушивания переговоров информационного характера: данные о связях объекта разработки, механизме встреч и передачи информации, местах хранения электронных носителей информации, денежных средств, о внешности, одежде, автотранспорте и т. д.

Эти данные имеют большое значение при проведении такого следственного действия, как обыск. Так, знание места хранения средств и орудий совершения киберпреступлений позволяет принять меры, препятствующие уничтожению (удалению) файлов на компьютере преступника, потере денежных средств, полученных в результате преступной деятельности;

2) результаты прослушивания переговоров, используемые для принятия решений при проведении мероприятий: данные о конкретном месте и времени встречи участников организованной преступной группы и др.;

3) результаты прослушивания переговоров, составляющие доказательственную базу (например, данные о логинах и паролях, инструментах кибератак).

Материалы с переговорами могут и должны быть применены при допросах подозреваемых, обвиняемых или свидетелей (время их применения при допросах следователь определяет самостоятельно, а при продолжении оперативной разработки преступной группы – по согласованию с инициатором разработки). Для допроса и приобщения к делу используются не оперативные сводки, а оформленные в соответствии с требованиями ст. 186 УПК РФ [2] протоколы прослушивания телефонных или иных переговоров, составленные оперативным сотрудником, и звукозаписи переговоров (в том числе на электронных носителях информации).

Еще более значимым для расследования уголовного дела является оперативно-разыскное мероприятие, связанное с **получением компьютерной информации** непосредственно *с сервера управления*[20], с помощью которого осуществляется основной объем преступных действий, в том числе отдаются команды на совершение несанкционированных финансовых транзакций. В зависимости от конкретных обстоятельств данное мероприятие может проводиться разово либо в режиме мониторинга. Полученная компьютерная информация может содержать сведения об использовании сервера для несанкционированного доступа к компьютерам пользователей, о наличии на нем вредоносных программ и их функциональных возможностях, о сетевых адресах, с которых осуществляется управление сервером, о совершенных через сервер хищениях в электронных платежных системах и др.

Компьютерная информация, полученная *с прокси-серверов*[21], содержит сведения об адресах серверов управления в конфигурационных файлах настройки, журнальные файлы сетевых подключений, среди которых могут быть сетевые адреса участников преступной группы, осуществлявших настройку и администрирование сервера, а также сетевые адреса компьютеров пользователей, зараженных вредоносной программой, которая через прокси-сервер взаимодействует с сервером управления.

Процесс проведения рассматриваемых оперативно-разыскных мероприятий связан с некоторыми **сложностями, связанными с вычленением из общей массы полученных сведений сообщений подозреваемых**. Эти сложности возникают прежде всего тогда, когда идет речь о многопользовательской системе, так как одно и то же идентификационное имя может быть доступно разным пользователям (как и один пользователь может скрываться под разными именами).

Вариантом решения данной проблемы следует признать совершенствование и развитие системы оперативно-разыскных мероприятий, а также создание передвижной лаборатории. В настоящее время на рынке отсутствуют какие-либо предложения по разработке универсальных центров работы специалиста по компьютерным программам. Представляется, что для обеспечения нормальной работы органов предварительного расследования и судов с электронными доказательствами достаточно в каждом субъекте Российской Федерации иметь такую передвижную лабораторию. Опыт использования подобных лабораторий уже имеется: они давно работают для проверки механических следов, взрывных устройств.

Таким образом, применение технико-криминалистических средств при проведении оперативно-разыскных мероприятий с точки зрения криминалистики имеет существенное значение в доказывании вины преступника. Следова-

---

[20] *Сервер управления* – сервер, дающий возможность удаленной настройки отдельных клиентов и их групп, формирования задач для групп клиентов и централизованного хранения их настроек, хранящий информацию о подключенных к нему узлах.

[21] *Прокси-сервер* (от англ. *proxy* – «представитель, уполномоченный»), часто просто *прокси*, *сервер-посредник* – промежуточный сервер (комплекс программ) в компьютерных сетях, выполняющий роль посредника между пользователем и целевым сервером.

тель может использовать только те доказательства, которые были получены законным путем. Поэтому технико-криминалистическое обеспечение специалистов и оперативных подразделений органов внутренних дел играет важную роль в организации взаимодействия при раскрытии и расследовании преступлений в сфере информационных технологий [76, с. 90].

Из изложенного становится очевидным, что залогом успешного доказывания по уголовному делу является оперативно-разыскное сопровождение следственной деятельности. Наибольшая же вероятность установления всех необходимых для предмета доказывания обстоятельств произошедшего возникает в том случае, когда уголовные дела о преступлениях, совершенных в сфере информационных технологий, возбуждаются в результате реализации оперативных материалов. Эти обстоятельства диктуют необходимость тесного взаимодействия оперативных работников и следователей на всех этапах расследования, в том числе и посредством создания следственно-оперативных групп.

Вопросы для самостоятельного изучения

1. Понятие и содержание обстоятельств, подлежащих проверке и доказыванию в процессе расследования преступлений в сфере информационных технологий.
2. Особенности возбуждения уголовного дела по материалам оперативно-разыскной деятельности при совершении преступлений в сфере информационных технологий.
3. Значение и производство специальных исследований при решении вопроса о возбуждении уголовного дела.
4. Криминалистические версии: понятие, виды и классификация. Их значение в раскрытии и расследовании преступлений в сфере информационных технологий.
5. Типичные следственные ситуации и действия следователя на первоначальном этапе расследования преступлений в сфере информационных технологий.
6. Основание и порядок приобщения результатов оперативно-разыскных мероприятий (аудио-, видеозаписи) в качестве доказательств при расследовании преступлений в сфере информационных технологий.
7. Взаимодействие следователя с оперативными подразделениями при проведении специальных технических мероприятий. Порядок использования в деле информации, полученной в ходе оперативно-разыскных мероприятий.

ГЛАВА 3. ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

§. 1. Тактические особенности производства следственных действий на первоначальном этапе расследования преступлений в сфере информационных технологий

Процесс расследования преступлений сфере информационных технологий обусловливает необходимость производства регламентированных УПК РФ следственных и иных процессуальных действий. При следственных действиях нужно соблюдать ряд правил, поскольку они регламентированы уголовно-процессуальным законом и их результаты могут формировать новые доказательства. *Тактические особенности их производства на первоначальном этапе расследования находятся в прямой зависимости от специфики следообразования и способа совершения преступления*.

Согласно результатам проведенного В. В. Коломиновым анализа следственной и судебной практики, **наиболее часто проводятся следующие следственные и иные процессуальные действия**:

1) осмотр места происшествия, осмотр предметов и документов (по 100 % уголовных дел);

2) допрос лиц, процессуальное положение которых определено (по 100 % уголовных дел). Большая часть – это допросы потерпевших и свидетелей, и в меньшей степени, при установлении виновных лиц, – допросы подозреваемых и обвиняемых, которые могут проводиться спустя значительный промежуток времени;

3) назначение и производство судебных экспертиз (по 100 % уголовных дел). Компьютерно-техническая экспертиза назначается в 100 % случаев, дактилоскопическая – в 60 %, технико-криминалистическая экспертиза документов – в 55 %, трасологическая – в 25 %, психологическая – в 10 %, иные виды экспертиз – в 5 % случаев;

4) получение образцов для сравнительного исследования (по 80 % уголовных дел);

5) предъявление для опознания (по 25 % уголовных дел);

6) обыск и выемка (по 90 % уголовных дел);

7) очная ставка (по 85 % уголовных дел);

8) следственный эксперимент и проверка показаний на месте (по 65 % уголовных дел);

9) снятие информации с технических каналов связи (по 25 % уголовных дел);

10) прослушивание телефонных и иных переговоров (по 5 % уголовных дел) и др. [30, с. 19].

В результате анализа следственной практики, касающейся преступлений в сфере информационных технологий, приходим к выводу о том, что при расследовании преступлений этой категории проводятся, в частности, такие следственные действия:

1) осмотр места происшествия;

2) допрос потерпевшего;

3) выемка и последующий осмотр средств электронно-вычислительной техники, предметов, материалов и документов [12, с. 120]. Проведение указанных следственных действий в ходе расследования преступлений в сфере информационных технологий имеет выраженную специфику, связанную с особенностями информационных объектов и необходимостью применения для их обнаружения и фиксации специальных программных и аппаратных средств [59, с. 81];

4) выемка почтово-телеграфной корреспонденции. Наложение ареста на корреспонденцию и выемка ее в почтово-телеграфных учреждениях;

5) допрос свидетеля;

6) допрос подозреваемого (если таковой установлен);

7) обыск на рабочем месте и по месту проживания подозреваемого;

8) назначение судебной экспертизы (чаще других это компьютерно-техническая [51, с. 20], радиотехническая, бухгалтерская экспертизы).

Нужно отметить, что, независимо от направленности следственного действия (поисковое или познавательное, связано с проверкой версии или развитием достоверного знания) и от того, какой способ собирания доказательственной базы является определяющим, всегда **деятельность следователя** по его производству **складывается из трех стадий**:

1) ознакомительно-ориентирующей;

2) непосредственного контактного или бесконтактного взаимодействия с объектом;

3) анализа полученных результатов, упаковки изъятых объектов, завершения процессуального оформления и т. д.

При проведении действий, в частности осмотре места совершения преступлений сфере информационных технологий, следователь сталкивается с **рядом проблем, которые обусловлены спецификой расследования преступлений данной категории**. Например, использование преступниками компьютерной техники и технологий определяет участие специалиста при проведении осмотра места происшествия как аксиому [50, с. 82]. Необходимость владения специальными знаниями обусловливает привлечение специалистов из различных областей информационных технологий, в частности инженерии по средствам связи, сетевому обслуживанию, а иногда возникает необходимость привлечения нескольких специалистов одновременно.

По мнению Ю. Г. Гаврилова, при проведении инструктажа следователю, как руководителю следственно-оперативной группы, необходимо убедиться в компетентности специалиста в указанной области знаний [39, с. 58].

Очевидно, что содействие специалиста оказывает следователю существенную помощь в раскрытии преступлений в сфере компьютерной информации, дает возможность эффективно расследовать дела данной категории. Целенаправленные, грамотные и четко спланированные действия следователя, специалиста и оперативных сотрудников, особенно на начальном этапе расследования, обеспечивают успех дальнейшего расследования преступлений, совершенных с использованием средств компьютерной техники.

Выделим несколько **рекомендаций по работе с компьютерно-техническими средствами и самой компьютерной информацией на месте происшествия**, *которые будут полезными при формировании доказательств, основанных на компьютерной информации*:

1) до начала следственных действий желательно иметь сведения, касающиеся марки и модели компьютера, средств связи, операционной системы, периферийных устройств, и любые другие сведения о технических средствах и программном обеспечении;

2) не стоит необдуманно включать или выключать световые приборы в осматриваемом помещении, торопиться и подключать к электросети или отключать от нее компьютерно-технические средства, подлежащие изъятию. Данные действия могут спровоцировать запуск программ по уничтожению либо модификации значимой информации;

3) категорически запрещается производить какие-либо операции с компьютерными средствами, расположенными на месте происшествия, до направления их на компьютерно-техническую экспертизу, и тем более работать на них после изъятия;

4) нельзя допускать к подлежащим изъятию техническим средствам владельца либо посторонних лиц, так как они могут зашифровать или удалить информацию;

5) необходимо принимать меры по установлению пароля доступа к защищенным программам и данным;

6) при активном вмешательстве сотрудников предприятия, стремящихся оказать противодействие следственно-оперативной группе, нужно отключить электропитание для всех компьютеров на объекте, надлежащим образом опечатать их и изъять вместе с магнитными носителями для дальнейшей отправки на компьютерно-техническую экспертизу;

7) если имеются подозрения, следует проверить технические средства на наличие программных «закладок» и вирусов, чтобы в дальнейшем суд не обвинил следствие в умышленном заражении технических средств вирусами при некомпетентном проведении следственных действий;

8) важно зафиксировать при помощи фотосъемки и промаркировать элементы компьютерной системы – это первые шаги при подготовке к изъятию и транспортировке. В частности, требуется выполнить снимки крупным планом всего компьютерного оборудования с нескольких сторон, в первую очередь спереди и сзади.

Фотографирование и маркирование элементов изымаемой компьютерной системы дает возможность в точности установить первоначальное состояние компьютерной техники при исследовании в лабораторных условиях. Это важно, например, для внешнего модема, где имеется ряд мелких переключателей, положение которых при транспортировке может измениться, что создаст дополнительные проблемы для экспертного исследования;

9) в присутствии понятых и других участвующих в следственном действии лиц нужно надлежащим образом изъять и опечатать все технические средства, сделав пояснительные бирки;

10) целесообразно изымать не только системные блоки, но и мониторы, магнитные носители, а также дополнительные периферийные устройства: принтеры, модемы, сканеры и т. п.;

11) важно тщательно проверять документацию, обращая внимание на рабочие и личные записи операторов электронно-вычислительной машины: часто именно в таких записях неопытных пользователей можно обнаружить коды, пароли и другую полезную информацию;

12) следует в списке сотрудников организации найти программистов и других специалистов в области информационных технологий. Не лишним будет установить их паспортные данные, адреса, контактные телефоны и места постоянной работы, если их деятельность в данном учреждении является временной;

13) необходимо записать данные всех лиц, находившихся в помещении в момент приезда следственно-оперативной группы, независимо от пояснения ими причин своего пребывания здесь;

14) наконец, нужно составить список всех сотрудников организации, имеющих доступ к компьютерной технике либо часто бывающих в помещении, где она находится.

Практикой выработаны следующие основные принципы, так называемые *«золотые» правила, детализирующие предложенные рекомендации, которыми следует руководствоваться следователю на месте преступления*, для совершения которого могли использоваться компьютеры и информационные технологии. Необходимо:

1) безотлагательно организовать охрану места происшествия;

2) принять неотложные меры для сохранности доказательств на электронных носителях: обеспечить бесперебойное питание компьютерного оборудования, исключить доступ посторонних лиц в помещение;

3) если компьютер выключен, оставить его выключенным, при этом сфотографировать (по правилам обзорной, узловой и масштабной фотосъемки) сам компьютер, место его расположения, вид спереди и сзади с кабелями и подключенными медиаустройствами;

4) если компьютер включен:

– сделать несколько снимков экрана, если что-то отображается на мониторе;

– если экран пуст, пошевелить мышью или нажать «пробел», что активизирует изображение на мониторе, после чего сфотографировать экран. Так как на компьютерной технике могут находится следы рук и микрообъекты, оставленные преступником, выполнять данные действия следует заранее проконсультировавшись со специалистом;

– не использовать компьютер, не производить никаких операций с файлами на нем;

– правильно завершить работу компьютера и подготовить его к транспортировке как вещественное доказательство;

5) в случае, когда имеются предположения о том, что компьютер уничтожает доказательства:

– немедленно выключить компьютер, выдернув кабель электропитания;

– если мобильный персональный компьютер не выключается, когда кабель электропитания от него отсоединен, найти и вынуть батарею автономного электропитания. Обычно она расположена на нижней панели и есть специальная кнопка или переключатель, позволяющий извлечь батарею. После того как батарея извлечена, нельзя возвращать ее на прежнее место и хранить в самом мобильном персональном компьютере: извлечение батареи предотвратит его случайный запуск;

6) сфотографировать пространство вокруг компьютерной техники, перед тем как перемещать что-либо из объектов (см. правила в рекомендациях выше);

7) для транспортировки:

– отметить и промаркировать кабели для последующей идентификации подключенных устройств;

– отключить все кабели и устройства от системного блока;

– упаковать комплектующие и транспортировать изъятое как хрупкий груз;

– изъять дополнительные устройства для хранения информации;

9) хранить все медиаустройства, включая системный блок, подальше от магнитов, радиоприемников и других потенциально опасных устройств;

10) изъять инструкции по эксплуатации, документацию и записи на бумаге;

11) при работе с компьютером, подключенным к компьютерной сети, кроме всего перечисленного, для надлежащей сохранности данных необходимо сначала отключить питание роутера или модема;

12) при работе с сервером компьютерной сети/сервером предприятия для надлежащей сохранности данных необходимо:

– сначала проконсультироваться у специалиста по компьютерной технике для дальнейшего оказания им помощи в осмотре;

– обеспечить охрану места происшествия и исключить доступ посторонних к объектам на месте происшествия, кроме специалиста, умеющего работать с компонентами компьютерных сетей;

– обеспечить бесперебойное питание сервера, так как его отключение может повлечь повреждение системы, причинение ущерба законной деятельности и, как следствие, привлечение к ответственности лица, проводящего расследование;

13) при работе с устройствами для хранения информации[22] для надлежащей сохранности данных необходимо:

– изъять инструкции по эксплуатации, документацию на бумаге;

– запротоколировать все действия, связанные с изъятием устройств для хранения информации;

– хранить их подальше от магнитов, радиоприемников и других потенциально опасных устройств;

14) при работе с карманными персональными компьютерами, мобильными телефонами и цифровыми фотокамерами, устройствами для хранения информации для надлежащей сохранности данных, помимо сказанного, необходимо:

---

[22] *Устройства для хранения информации* предназначены для хранения компьютерной информации, получаемой с электронных устройств, могут различаться по объему памяти.

– учитывать, что карманные персональные компьютеры, мобильные телефоны и цифровые фотокамеры могут содержать информацию во встроенной памяти или на отдельно подключаемых медианакопителях, поэтому нужно изъять дополнительные устройства для хранения информации, например, карты памяти: memory stick, compact flash и т. п. По общему правилу, все действия, связанные с изъятием мультимедийных устройств и их компонентов, как и любых объектов, должны быть процессуально оформлены соответствующим протоколом следственного действия, в котором фиксируется его ход [60, с. 207];

– поддерживать устройство в заряженном состоянии;

– если устройство не может поддерживаться в заряженном состоянии, организовать исследование специалистом до того, как батарея автономного питания устройства разрядится, так как иначе информация может быть потеряна.

Что касается **изъятия электронных носителей информации и копирования с них информации**, то важно учитывать, что при производстве по уголовным делам, указанным в ч. 4.1 ст. 164 УПК РФ, оно *не допускается*, так как это влечет применение необоснованных мер, которые могут привести к приостановлению законной деятельности юридических лиц или индивидуальных предпринимателей, *за исключением следующих случаев*:

1) вынесено постановление о назначении судебной экспертизы в отношении электронных носителей информации;

2) изъятие электронных носителей информации производится на основании судебного решения;

3) на электронных носителях содержится информация, полномочиями на хранение и использование которой владелец носителя не обладает, либо которая может быть использована для совершения новых преступлений, либо копирование которой, по заявлению специалиста, может повлечь за собой ее утрату или изменение [2, ст. 164].

Согласно общим правилам, закрепленным в ст. 164.1 УПК РФ, электронные носители информации изымаются в ходе производства следственных действий *с участием специалиста*.

По ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалистом, участвующим в следственном действии, в присутствии понятых осуществляется копирование информации с изымаемых носителей на другие электронные носители информации, предоставленные законным владельцем или обладателем содержащейся на изымаемых носителях информации.

Электронные носители, содержащие скопированную информацию, передаются законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации.

О копировании информации и о передаче электронных носителей информации, ее содержащих, законному владельцу или обладателю содержащейся на них информации в протоколе следственного действия делается запись.

Следователь в ходе следственного действия вправе скопировать информацию, содержащуюся на электронном носителе. В протоколе следственного действия должны быть указаны примененные при этом технические средства, порядок их применения, электронные носители информации, к которым эти средства были применены, и полученные результаты. К протоколу прилагаются электронные носители, содержащие скопированную информацию [2, ст. 164.1].

Уголовно-процессуальный закон предписывает **обязательное участие понятых при осмотре места происшествия**, однако, как указывают некоторые авторы, те должны обладать познаниями в области компьютерной техники и технологий [49, с. 5], что на практике трудно представить, в частности, из-за нередкой неотложности производства такого следственного действия. Проблема в том, что понятые, не обладающие специальными познаниями, могут позднее заявить о непонимании происходившего при производстве следственного действия.

Одно из самых распространенных следственных действий при расследовании любого преступления – **допрос**. Не являются исключением и преступления в сфере компьютерной информации.

При производстве допроса следователю необходимо избирать тактику действий в зависимости от механизма совершения преступления в сфере компьютерной информации [77, с. 27].

Р. С. Белкин верно описал *допрос* как процессуальное действие, заключающееся в получении показаний (информации) о событии, ставшем предметом уголовного судопроизводства, лицах, проходящих по делу, причинах и условиях, способствовавших совершению и сокрытию преступления [15, с. 64].

Как и иные следственные действия при расследовании преступлений в сфере информационных технологий, допрос обладает определенными особенностями.

На выбор тактики производства допроса влияет достаточность объема информации о расследуемом преступлении. Такие сведения следователь получает из различных источников, как процессуальных (результаты иных проведенных следственных действий), так и непроцессуальных (результаты оперативно-разыскных мероприятий). Также при установлении обстоятельств совершения преступлений в сфере информационных технологий необходимы знания об особенностях механизма преступления, возможных орудиях и средствах его совершения.

Бесспорно, залогом успешно проведенного допроса является тщательная подготовка к его производству.

На подготовительной стадии обязательно использование полученных в ходе доследственной проверки материалов.

Н. Г. Шурухнов отмечает, что «…первоначальный допрос на предварительном следствии лица, от которого во время проведения предварительной проверки были получены объяснения, будет являться повторным изложением события, интересующего следствие. Данное обстоятельство имеет определенное значение, так как предварительная проверка создает благоприятную базу для до-

проса на предварительном следствии. Что касается недобросовестных участников процесса, оказывающих противодействие расследованию, то первоначальное получение объяснений от них дает возможность заранее определить позицию, которую займет это лицо на допросе, и соответствующим образом к этому подготовиться» [79, с. 52].

Перечисленные особенности также оказывают влияние на выбор следователем тактических приемов при производстве допроса.

Нельзя забывать, что допросы потерпевшего и свидетеля по делам о преступлениях в сфере информационных технологий отличаются от допросов подозреваемого и обвиняемого.

Общепринято при допросе потерпевшего (свидетеля) выяснять следующую информацию:

– о наличии у него специальных знаний о технических характеристиках электронно-вычислительной машины;

– о технических средствах, которыми пользовалось допрашиваемое лицо;

– об умениях и способностях допрашиваемого в области компьютерной информации;

– о наличии знаний о программных средствах, установленных на компьютере допрашиваемого лица;

– о фирме-провайдере, которые предоставляли абоненту услуги сети Интернет;

– о том, из каких источников допрашиваемый получил информацию о преступных действиях лица;

– о том, как осуществлялось общение (контактное взаимодействие) между потерпевшим или свидетелем и преступниками;

– о том, был ли установлен визуальный контакт между ними и при каких условиях, сможет ли он опознать подозреваемых.

Приведенный перечень не является исчерпывающим и зависит от исходной следственной ситуации. Особенно скрупулезно следует подойти к допросу системных администраторов предприятий и организаций. Готовясь к такому допросу, следует иметь в виду, что, с одной стороны, они могут состоять в сговоре с лицами, совершившими преступление, с другой – могут обладать большим объемом информации о нем, и с учетом того, что в ходе расследования могут быть выявлены нарушения с их стороны в обслуживании компьютерно-технических средств, приведшие к совершению преступлений в сфере информационных технологий, они же могут давать ложные показания.

Для успешного проведения допроса подозреваемого необходимо тщательно изучить материалы уголовного дела, особенности его личности, способы совершения преступления, технические средства и компьютерные программы которые им использовались, а также иные доказательства, указывающие на виновность конкретного лица.

Необходимо отметить, что в ходе допроса подозреваемого могут складываться следующие следственные ситуации:

1) лицо совершившее преступление объясняет факт неправомерного доступа к компьютерной информации некриминальными причинами (случайностью, стечением определенных обстоятельств, посторонним воздействием и т. п.).

2) подозреваемый дает показания о неправомерном доступе к компьютерной информации как о факте, который свершился при отсутствии преступного умысла либо в силу незнания российского законодательства в сфере информационной безопасности.

В процессе допроса лица, подозреваемого в совершении преступления в сфере информационных технологий, следует принимать во внимание следующие моменты:

– на эффективность допроса во многом влияет то, в каком психологическом состоянии пребывает допрашиваемый, осознает ли свою вину, намерен ли дать правдивые показания;

– в ходе подготовки к допросу подозреваемого в совершении преступления, при наличии реальной возможности, следователю стоит получить рекомендацию от психолога в целях формирования наиболее эффективной тактики допроса;

3) рекомендуется проконсультироваться со специалистов в области высоких технологий, что даст возможность принять во внимание характерные особенности конкретного преступления в рассматриваемой области.

Если подозреваемый использует специальные термины, целесообразно в конце допроса (а иногда и по ходу) предложить ему пояснить их значение. Дело в том, что специалисты в различных отраслях компьютерных технологий одни и те же слова могут толковать с разных точек зрения, иногда отличных от общеизвестных. Кроме того, некоторые начинающие хакеры, желая показать свои «знания» в сфере информационных технологий, используют термины неправильно, не понимая их смысла. Поэтому допрашиваемому необходимо предложить существующие как в профессиональном языке программистов, так и в жаргоне (компьютерном сленге) словарные определения, с которыми он либо согласится, либо предложит свою формулировку. При этом следует помнить, что наводящие вопросы в ходе допроса не допускаются [23, с. 99].

При изобличения подозреваемых в преступной деятельности хорошие результаты дает правильное применение тактических приемов, и их использование на основе данных, полученных при проведении оперативно-разыскных мероприятий и следственных действий (осмотр места происшествия, обыск). Следователю необходимо корректно комбинировать и использовать тактические приемы ведения допроса в целях снижения или нейтрализации негативного психологического состояния и усиления и поддержки позитивного. Умелое применение сведений оказывает психологическое воздействие на допрашиваемого и позволяет получить правдивые показания в ходе допроса.

Если допрос подозреваемого проводится сразу после проведенного у него обыска, то целесообразно выяснить у него сведения об используемых средствах сокрытия криминалистически значимой компьютерной информации: паролях, либо иных данных для получения доступа к зашифрованным областям данным

и заблокированным устройствам. Важно получить эти данные в тот момент, пока он еще не выработал защитную тактику, направленную на противодействие расследованию.

Подводя итог, можно прийти к выводу о том, что при производстве допроса по делу о преступлении в сфере информационных технологий следователю необходимо обладать определенным объемом знаний, позволяющих ориентироваться в данной области. Рекомендуется консультация специалиста, что позволит тщательно подготовиться к проведению допроса.

§ 2. Применение специальных знаний при расследовании преступлений в сфере информационных технологий

Несмотря на повышенное внимание со стороны исследователей к расследованию преступлений, связанных с компьютерной техникой, тактика применения специальных знаний в области высоких технологий остается не до конца изученной. Имеется целый ряд рекомендаций по вопросам назначения и проведения экспертиз компьютерной техники и информации, часто они сложны для самостоятельного использования лицами, проводящими расследование. Соответственно, многие авторы оправданно отмечают актуальность привлечения специалистов, о чем мы уже говорили.

Таким образом, отсутствие необходимого объема знаний, выходящих за рамки профессиональных юридических знаний следователей и общих знаний информационных технологий, в случае необходимости восполняется привлечением к расследованию субъектов, для которых данные знания являются профессиональными. Такие знания в уголовно-процессуальном законодательстве называются *специальными*. Преимущество специальных знаний заключается в том, что они фактически открывают неограниченные возможности для достоверного применения достижений науки и техники при расследовании преступлений в законодательно установленном порядке.

Имеющиеся сегодня методические рекомендации по выявлению и расследованию правоохранительными органами преступлений в области информационных технологий не могут отражать всех особенностей деятельности преступников. Корректное **представление о формах применения специальных знаний в уголовном судопроизводстве** дает возможность использовать их с учетом разработанных научных рекомендаций и последних практических наработок.

Роль экспертных подразделений заключается в оказании методической помощи, экспертном сопровождении при расследовании преступлений, поиске и установлении значимой для расследования информации. В экспертных подразделениях МВД России производятся судебные компьютерно-технические экспертизы и исследования, имеется оборудование, позволяющее анализировать информацию на различных носителях, но современные достижения на рынке коммуникаций, их опережающее развитие по отношению к созданию систем безопасности приводят к постоянному появлению новых рисков и угроз, поэтому важно своевременно проводить обучение сотрудников, обновлять материальную базу лабораторий, искать современные методы исследования информационных

объектов, использовать информационное пространство Интернета для отслеживания очередных видов угроз.

При *подготовке (переподготовке) специалистов, занимающихся выявлением, пресечением, расследованием преступлений*, совершаемых с использованием информационно-коммуникационных технологий, следует обращать внимание на то, что они должны:

1) иметь представление о видах и механизмах преступлений, совершаемых с использованием информационно-коммуникационных технологий;

2) знать перечень объектов (носителей) информации, уметь правильно включать оборудование и завершать его работу, производить изъятие и упаковку с целью сохранности информации;

3) знать механизмы передачи и места хранения информации на электронных носителях, способы передачи информации в локальной сети и сети Интернет;

4) иметь представление о сетевых технологиях (локальная сеть, сеть Интернет и т. п.), четко разбираться в терминологии сетевых построений;

5) уметь проводить осмотр места происшествия и строить план проведения осмотра в зависимости от характера преступления, четко представлять, специалисты какого профиля могут дополнительно понадобиться при проведении осмотра (системный администратор, бухгалтер, специалист по видеооборудованию, инженер-электрик, специалист в области спутниковой связи и т. д.);

6) уметь формулировать вопросы при назначении судебной компьютерной экспертизы;

7) уметь интерпретировать результаты проведенной судебной компьютерной экспертизы (осмотра места происшествия);

8) уметь пользоваться ресурсами сети Интернет для поиска необходимой справочной информации.

В этой связи *применение специальных знаний* специалиста и эксперта в процессе расследования преступлений в области компьютерной информации *должно строиться на конкретных требованиях*, среди которых:

1) соблюдение норм процессуального права;

2) достоверность, допустимость и относимость получаемой с помощью эксперта или специалиста доказательственной информации;

3) соответствие концептуальному уровню развития научных знаний и апробированным методикам их применения (с учетом таких направлений и подходов, как синергетический, ситуационный (ситуалогический), системный) [41, с. 125].

С позиции расследования преступлений в сфере компьютерной информации толкование термина «специальные знания» может быть более узким, когда он трактуется как исключительно знания в определенных рамках, обладающие углубленным систематизированным характером, в частности знания об устройстве и функционировании какого-либо вида компьютерной техники или каких-либо программных продуктов. Таким образом, привлекая специалистов к участию в следственных действиях, назначая экспертизу, *не следует забывать о предметной специализации экспертов и специалистов*.

Итак, *специальные знания при расследовании преступлений в рассматриваемой сфере* представляют собой углубленные систематизированные знания в области информационных технологий и компьютерной техники, доступные относительно узкому кругу профессионалов, а также практические навыки применения данных знаний, выработанные в процессе профессиональной деятельности [48, с. 100].

Рассматривающиеся в пособии преступления являются преступлениями в сфере высоких технологий, в которой следователь, как мы уже не раз подчеркивали, в большинстве случаев не имеет достаточно глубоких познаний. Соответственно, без специальной помощи он может совершить непоправимые ошибки в процессе осмотра технической аппаратуры, снятия необходимых данных и/или их изъятия.

Преступления, которые связаны с электронными документами и компьютерными средствами, нередко обладают высоким уровнем латентности, не оставляют видимых следов и сложны с позиции раскрытия и собирания доказательственных сведений из-за сложности объектов – носителей данных сведений, широкого использования средств удаленного доступа и целого ряда иных причин. В ходе расследования таких преступлений участие специалиста в области разработки и применения современных информационных технологий является необходимым вследствие того, что даже незначительные неквалифицированные действия с компьютерной системой могут повлечь за собой потерю ценных разыскных и доказательственных сведений, а на их восстановление может уйти много времени.

Специалист привлекается к осуществлению следственных действий для более верного уяснения вопросов пользования конкретными компьютерными средствами в определенной следственной ситуации, оказания помощи следователю в подборе понятых, в качестве которых следует привлекать лиц, разбирающихся в компьютерной технике, а также использует данные компьютерные средства в целях обнаружения, фиксации и изъятия данных о совершенном преступлении в области компьютерной информации.

Участие специалиста может стать необходимым элементом почти на всех этапах расследования преступлений, связанных с применением средств компьютерной техники: начиная с этапа возбуждения (для получения достаточных сведений, указывающих на признаки преступления) и заканчивая рассмотрением дела в суде (в частности, для разъяснения значения сделанных экспертом выводов).

Отметим, что *в ситуациях, когда появляется необходимость установления факта нахождения какой-либо информации на машинном носителе данных*, назначение и осуществление судебной экспертизы необязательно. Факт нахождения определенной информации, существенной для уголовного дела, может быть зафиксирован в ходе следственного осмотра с участием специалиста. Подчеркнем, что при указанном следственном действии участие специалиста и сведущих понятых обязательно для того, чтобы исключить возможные в будущем заявления заинтересованных лиц об изменениях, либо о внесении иных данных следователем в процессе осмотра сведений, содержащихся в компьютерной системе, на машинных носителях данных.

Для участия в осмотре специалиста следует привлекать тогда, когда исследование самого объекта, изменений в нем, сопряженных с совершением преступления, а также обнаружение и фиксация следов и вещественных доказательств подразумевают использование либо знаний, умений, которых у следователя нет, либо технических средств, по применению которых следователь не имеет необходимых умений или использование которых в ходе осмотра отвлечет его от выполнения иных, таких же важных и неотложных при осмотре, действий.

В качестве основной формы применения специальных знаний при расследовании и судебном рассмотрении уголовных дел выступает **судебная экспертиза**.

Вид судебной экспертизы, в процессе которой применяются специальные знания в области компьютерной техники и информационных технологий, начал становление примерно с середины 1990-х, когда начали проводиться отдельные уникальные исследования. Появление нового рода судебной экспертизы было вызвано растущими потребностями следственной практики.

На начальной стадии развития отдельные ученые выделяли два вида такой экспертизы:

1) техническая экспертиза компьютеров и их комплектующих, ориентированная на исследование конструктивной специфики и состояния компьютера, его периферийных устройств, магнитных носителей, компьютерных сетей, а также причин появления сбоев в работе перечисленного оборудования;

2) экспертиза данных и программного обеспечения, производимая для исследования данных, которые хранятся в компьютере и на других носителях информации [64, с. 31].

Наиболее актуальной стала *классификация видов компьютерно-технической экспертизы*, разработанная Е. Р. Россинской и А. И. Усовым, выделившими четыре вида:

1) аппаратно-компьютерная экспертиза;

2) программно-техническая экспертиза;

3) информационно-компьютерная экспертиза (данных);

4) компьютерно-сетевая экспертиза [41, с. 121].

По мнению отдельных исследователей [40, с. 78; 27, с. 52], данная классификация принята за основу при описании судебных экспертиз, назначаемых для исследования средств компьютерной техники и информации, большинством ученых, занимающихся изучением вопросов борьбы с преступностью в области компьютерной информации.

Помимо того, что в ходе расследования при назначении определенного вида экспертизы необходимо четко понимать ее задачи, важно правильно задавать вопросы эксперту, а точнее их формулировать (правильно заданный вопрос – это 90 % правильного ответа).

В силу нехватки определенных специальных знаний это вызывает у следователей (дознавателей) определенные сложности, поэтому рассмотрим *требования, предъявляемые к вопросам*.

Вопросы, поставленные перед экспертом должны быть:

– краткими и конкретными;

– не допускающими двоякого толкования;

– в случае поисковых запросов – не содержащими орфографических или иных ошибок (опечаток), неточно заданными.

Так, если поисковый запрос подразумевает указание фамилии, имени, отчества или названия организации, то логично приводить данные как в полном, так и в сокращенном виде (например: Иванов Александр Иванович и Иванов А. И., отдел технического сопровождения «Спектр» и ОТС «Спектр»);

– не носящими справочный или правовой характер (например, некорректны вопросы типа «Каково назначение данного устройства?», «Является ли представленный объект игровым (лотерейным) аппаратом?» и т. п.);

– относящимися к компетенции эксперта в компьютерно-технической области;

– могущими быть решенными с помощью оборудования, имеющегося в распоряжении экспертно-криминалистического центра.

В. И. Вараксин в этой связи отмечает, что *одной из ошибок следователя является назначение экспертизы без предварительной консультации с экспертным учреждением*. Как следствие, производство экспертизы ведется не в полном объеме или оказывается невозможным либо лицо, осуществляющее экспертное исследование, может выйти за пределы своей компетенции и представить ошибочное (необоснованное) заключение [47, с. 78].

Для правильной постановки вопроса до назначения экспертизы желательно провести консультацию со специалистом (экспертом), кратко разъяснив ему обстоятельства совершения преступления и описав объекты исследования, в некоторых случаях для получения данных о следовой картине логично провести предварительное изучение информации, содержащейся на объекте, и уже по полученным результатам строить цепочки вопросов, конкретизировать их.

Предметом судебной компьютерно-технической экспертизы являются факты, события и обстоятельства, устанавливаемые в процессе исследования информационных процессов компьютерных средств: создания, сбора, обработки, накопления, хранения, поиска, распространения, использования информации.

Родовой (видовой) объект судебной компьютерно-технической экспертизы – определенная категория технических, аппаратных и программных средств, обладающих общими признаками, относящихся к компьютерным средствам и предназначенных для автоматической обработки электронной информации.

К числу аппаратных *объектов* компьютерно-технической экспертизы относятся:

– персональные компьютеры, ноутбуки, планшеты;

– периферийные устройства (любые дополнительные и вспомогательные устройства, которые подключаются к компьютеру для расширения его функциональных возможностей);

– сетевые аппаратные средства (серверы, рабочие станции, активное оборудование, сетевые кабели и т. д.).

К числу интегрированных систем (органайзеров) относятся:

– телефоны и смартфоны (карты памяти различных классов, видов и поколений);

– магнитные носители информации (накопители на жестком диске, USB-, флеш-накопители и т. д.);

– платежные банковские карты с магнитной полосой или чипом;

– встроенные системы на основе микропроцессорных контроллеров (иммобилайзеры, транспондеры, круиз-контроллеры и т. п.);

– любые комплектующие всех вышеуказанных компонентов.

Программные объекты компьютерно-технической экспертизы:

– системное программное обеспечение;

– вспомогательные программы-утилиты;

– средства разработки и отладки программ;

– прикладное программное обеспечение.

Информационные объекты (данные):

– текстовые и графические документы, изготовленные с помощью компьютерных средств;

– данные в форматах мультимедиа;

– информация в форматах баз данных и других приложений, имеющая прикладной характер.

В качестве *общих задач*, решаемых компьютерно-технической экспертизой, рассматриваются:

– установление свойств и вида представления информации в компьютерной системе при ее непосредственном исследовании;

– определение фактического состояния информации, выяснение наличия или отсутствия в ней отклонений от типового объекта экспертизы (например, имеются ли вредоносные включения, нарушение целостности и т. д.);

– установление первоначального состояния информации на носителе данных;

– определение условий изменения свойств исследуемой информации (например, модификация или внесение изменений в содержимое файла либо в запись на магнитный носитель пластиковой карты и т. п.);

– определение механизма и обстоятельств события (дела), установление отдельных этапов (стадий, фрагментов) события по имеющейся на носителе данных информации или ее копиям (например, подготовка нескольких копий делового письма и его рассылка факсимильной программой в разные адреса);

– определение времени (периода), хронологической последовательности воздействия на информацию (например, установление стадий подготовки изображений денежных знаков, оттисков печатей т. п.);

– установление причинно-следственной связи между имевшими место манипуляциями с компьютерной информацией и наступившими последствиями (например, связи между удалением информации и нарушением работоспособности компьютерной системы).

К *специальным задачам* компьютерно-технической экспертизы можно отнести отождествление содержания файла с данными в копии исследуемого файла либо в представленном документе (в том числе в бумажной копии) в комплексе

с технико-криминалистическим исследованием документов). Групповая принадлежность может устанавливаться при поиске общего источника происхождения информации на носителях данных компьютерной системы, а также при определении класса, вида и типа программного обеспечения, при помощи которого были порождены (созданы) исследуемые данные.

Основные вопросы, решаемые компьютерно-технической экспертизой:

1) исправны ли представленные на исследование объекты;

2) имеются ли на жестких дисках персональных компьютеров и на других представленных на исследование носителях информации файлы (фрагменты файлов, в том числе и среди удаленных), содержание которых полностью или частично идентично представленному на экспертизу объекту;

3) имеется ли на жестких дисках персонального компьютера и на других представленных на исследование носителях информации программное обеспечение, с помощью которого могли быть изготовлены представленные объекты;

4) имеются ли на жестких дисках персонального компьютера и на других представленных на исследование носителях информации какие-либо программные средства для несанкционированного доступа и расшифровки учетных данных для соединения с сетью Интернет;

5) имеется ли на жестких дисках персонального компьютера программное обеспечение для подключения и работы в сети Интернет, и если да, то имеются ли следы соединений и работы в Интернете, каковы дата и время создания соединений;

6) имеются ли следы соединения и работы в сети Интернет с использованием учетных данных ********** (логины и пароли для соединения с сетью Интернет, установленные в ходе следствия);

7) каковы учетные данные (логины и пароли) для соединения с сетью Интернет на представленных на исследование носителях информации;

8) имеются ли на жестких дисках персональных компьютеров и на других представленных на исследование носителях информации вредоносные программы и средства удаленного администрирования, сессии и log-файлы их работы;

9) соответствуют ли представленные на исследование сотовые телефоны требованиям сертификатов соответствия Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации;

10) каковы регистрационные данные программного обеспечения, установленного на жестких дисках представленного на исследование персонального компьютера, имеются ли признаки его контрафактности;

11) имеются ли признаки контрафактности программных продуктов, содержащихся на представленных носителях (компакт-диски различных форматов, гибкие магнитные диски и т. п.) [38, с. 63].

В зависимости от следственной ситуации, которая складывается на момент расследования, *типовые вопросы, выносимые на разрешение компьютерно-технической экспертизы*, логично разделить на четыре условных блока.

1. *Поиск информации*.

В данном случае речь идет о поиске на компьютерном носителе файлов, документов, изображений, сообщений и иной информации, относящейся к делу, в том числе в неявном (удаленном, скрытом, зашифрованном) виде. При назначении экспертизы рекомендуется не конкретизировать вид и содержание искомой информации. Эксперт вполне может самостоятельно решить, относится ли тот или иной текст, изображение или программа к делу. Типовой задачей поиска информации на носителе является поиск файлов, содержащих информацию, сходную или аналогичную представленной в документе (на изображении).

Типовые вопросы:

1) имеются ли на представленном носителе информации файлы (указать какие: тип файла, расширение, имя файла и т. д.);

2) имеются ли на представленном носителе файлы, содержащие ключевые слова (ключевые фразы): (указать, какие именно, например, название фирмы, ФИО и т. п.);

3) какова дата последней модификации файла, каковы свойства документа, содержащегося в обнаруженном файле;

4) содержатся ли на представленном носителе информации информационные базы программы (указать какой именно, например «1С»);

5) какая информация содержится на представленной банковской карте с магнитной полосой (чипом);

6) имеются ли на представленном носителе информации файлы, содержащие изображения (указать, какие именно);

7) имеются ли на представленном носителе информации файлы, содержащие изображения, сходные или аналогичные представленным образцам.

2. *Исследование следовой картины*.

В данном случае речь идет о поиске цифровых следов различного рода действий, совершаемых с компьютерной информацией. Вопросы лучше формулировать не про следы, а про действия. Когда компьютер используется как средство доступа к информации, находящейся в ином месте, и когда доступ к информации осуществляется на этом компьютере, в обоих случаях остаются так называемые цифровые следы – следы в виде компьютерной информации. Компьютерная экспертиза может определить, когда, при каких условиях и каким образом осуществлялся доступ. Кто его осуществлял, компьютерная экспертиза определить не может. Лишь в некоторых случаях эксперту удается обнаружить некоторые сведения о пользователе компьютера.

Действия, которые оставляют следы на компьютере или на носителе информации, включают: доступ к информации, ее просмотр, ввод, изменение, удаление, любой другой вариант обработки или хранения данных, а также удаленное управление этими процессами.

Типовые вопросы:

1) имеются ли следы работы пользователя в сети Интернет. Если да, то за какие периоды времени;

2) имеются ли следы редактирования, создания, распечатки документа (предоставляется документ или его распечатка);

3) имеются ли следы работы программного обеспечения (указать какого именно). Если да, то имеются ли файлы, созданные (или которые могли быть созданы, редактированы) с использованием данного программного обеспечения;

4) имеются ли следы удаленного администрирования на представленном носителе информации.

3. *Определение временных интервалов*.

В данном случае речь идет об установлении времени и последовательности совершения пользователем различных действий.

Благодаря наличию в компьютере внутренних энергонезависимых часов и создании в различных местах временных меток, становится возможным определить, когда и в какой последовательности пользователь производил различные действия.

Так, если внутренние часы компьютера были переведены вперед или назад (в том числе неоднократно), все равно имеется возможность восстановить правильное время и правильную последовательность событий. Перевод часов компьютера сам по себе оставляет следы. А если еще было и сетевое взаимодействие, то есть возможность сопоставить моменты событий, зафиксированные данным компьютером, с событиями, установленными по иным источникам, и выяснить факт сдвига внутренних часов.

Задача выполнима даже в том случае, если системный блок, содержащий внутренние часы, не находится в распоряжении эксперта. Только по носителю информации (например, накопителю на жестком магнитном диске) можно получить сведения о последовательности событий. Чем больше информации на носителе, тем полнее будет восстановленная картина.

Отмечают даже такую экзотическую задачу, как подтверждение (опровержение) алиби подозреваемого, который утверждает, что в определенное время работал за компьютером. В этом случае, хотя речь не идет о компьютерном преступлении, для проверки алиби потребуется судебная компьютерная экспертиза.

Типовые вопросы:

1) имеются ли на жестких дисках персонального компьютера и на других, представленных на исследование носителях информации файлы (фрагменты файлов, в том числе и среди удаленных), содержащие информацию, аналогичную представленным на исследование образцам (либо сходную с образцами), и если да, то каковы дата и время создания (последней модификации) обнаруженных файлов;

2) имеются ли на жестких дисках персонального компьютера и на других представленных на исследование носителях информации файлы (фрагменты файлов, в том числе и среди удаленных), содержащие изображения печатей (штампов, денежных купюр и т. п.), сходные или аналогичные представленным на исследование образцам, и если да, то каковы дата и время создания (последней модификации) обнаруженных файлов.

4. *Исследование программного обеспечения, установленного на представленном носителе информации, и исследование дистрибутивов, содержащихся на нем*.

В рамках данного вида исследования устанавливается наличие того или иного программного обеспечения на представленном носителе информации, его версия, релиз, регистрационные данные. Следует отметить, что вопросы о «контрафактности» или о «признаках контрафактности» носят правовой характер и выходят за рамки компетенции судебной компьютерной экспертизы. В ее рамках эксперт может обнаружить отличия версии установленного (представленного) образца программного обеспечения от лицензионного образца. Следует отметить, что для сравнения необходим инсталляционный пакет программного обеспечения той же версии, релиза, что и для исследуемого образца программного обеспечения. При назначении исследования следует избегать общих вопросов типа «Какое программное обеспечение установлено на представленном носителе информации?» или «Какие программные продукты корпорации Microsoft (Adobe, Corel и т. д.) установлены?» или «Содержатся ли дистрибутивы программ Microsoft (Adobe, Corel и т. д.)?».

Типовые вопросы:

1) установлено ли на представленном носителе информации программное обеспечение (или его дистрибутивы) корпорации Microsoft: Microsoft Windows, Microsoft Office и др.? Если да, то какое именно;

2) каковы регистрационные данные, версия, релиз программного обеспечения (указывается, какого именно), дата и время его установки?

Иногда в процессе расследования преступлений в сфере информационных технологий нет возможности провести экспертное исследование в лаборатории, например, если стало известно, что компьютер обладает высоким уровнем защиты или что этот компьютер является важным элементом корпоративной сети компании и его изъятие невозможно без причинения ей существенного ущерба.

В процессе производства *ситуационной компьютерно-технической экспертизы* в здании, где находится юридическое лицо, работником которого является подозреваемый (обвиняемый) в совершении преступления в сфере компьютерной информации, следователь должен обеспечить эксперту максимальный доступ к необходимым данным. Если говорить о крупной фирме, то существует вероятность того, что у нее имеется служба или департамент информационной безопасности в составе службы общей безопасности. Данное подразделение традиционно обладает практически всеми данными об информационно-компьютерных ресурсах компании и может существенно облегчить работу эксперту.

Важно помнить, что, так как объектом судебной компьютерно-технической экспертизы является информация, зафиксированная на различных носителях с энергонезависимой памятью, *изъятие носителей информации производится с соблюдением необходимых правил*, гарантирующих сохранность информации, которые подробно рассматривались нами в первом параграфе третьей главы.

Напомним, что перед изъятием устройства необходимо обесточить компьютер, но в некоторых случаях (например, при сетевых киберпреступлениях, когда на момент осмотра и изъятия устройство включено) перед обесточиванием

и изъятием необходимо провести осмотр и зафиксировать все запущенные процессы (исполняемые программы, открытые веб-страницы и документы), либо описав их, либо произведя фото-, видеосъемку экранов с запущенными приложениями и экранов сетевых настроек. Это обусловлено тем, что многие сетевые процессы не отражаются в журналах (особенно программы хакерского направления) и после выключения устройства следовая картина будет неполной, а в некоторых случаях может и вовсе отсутствовать. При изъятии объектов следует обращать внимание на наличие каких-либо записей на отдельных листах, в тетрадях, в записных книжках: многие злоумышленники прячут информацию, используя средства криптографической защиты (BestCrypt, PGP и т. д.).

Чаще всего снять серьезную криптографическую защиту в условиях лаборатории экспертно-криминалистического подразделения не получается, что делает невозможным проведение дальнейшего исследования.

Следует отметить, что наличие самого современного оборудования и работа специалистов высокого класса не всегда приводят к 100-процентному результату при расследовании и раскрытии преступления. Очень *важно наладить взаимодействие в цепочке эксперт – следователь* для определения объектов, границ исследования, составления вопросов и правильной интерпретации полученных выводов эксперта.

Кроме того, исследование компьютерной информации часто носит *комплексный характер*, так как при его проведении привлекаются эксперты нескольких специальностей (специализаций). Состав экспертной комиссии часто можно определить только по результатам ознакомления экспертов с обстоятельствами дела и имеющимися материальными носителями информации. В этой связи может возникнуть *необходимость в предварительном экспертном исследовании поступивших объектов и их экспертной классификации*.

Таким образом, среди основных задач компьютерно-технической экспертизы в целом можно обозначить следующие:

1) установление первоначального состояния информации на носителе данных;

2) установление свойств и вида представленной информации;

3) определение условий внесения изменений в содержимое файла и т. п.;

4) определение механизма и обстоятельств определенного события (факта);

5) установление отдельных этапов (стадий, фрагментов) события по имеющейся на носителе данных информации или ее копиям;

6) определение времени (периода) и хронологической последовательности воздействия на информацию;

7) установление причин неисправности носителя данных;

8) установление причин отсутствия доступа к информации;

9) исследование однотипной и разнотипной информации с двух разных носителей и т. д.

Подводя итог, следует отметить, что возможности технико-криминалистических средств и методов, используемых на базе компьютерной техники,

имеют значительный потенциал, позволяющий решать множество задач при раскрытии и расследовании преступлений. Учебное пособие раскрывает лишь малую часть теоретических и практических возможностей применения специальных познаний в правоохранительной деятельности, однако уже существующие разработки и алгоритмы действий по применению компьютерной информации должны, на наш взгляд, более активно использоваться в раскрытии и расследовании преступлений в сфере информационных технологий. При этом положительная перспектива очевидна.

Вопросы для самостоятельного изучения

1. Тактика следственного осмотра при расследовании уголовных дел о преступлениях в сфере информационных технологий. Особенности фиксации результатов следственного осмотра.

2. Особенности осмотра места происшествия в зависимости от объекта: осмотр электронных носителей информации, осмотр работающего компьютера, осмотр неработающего компьютера, осмотр предметов и документов.

3. Тактические особенности задержания подозреваемого и проведения личного обыска при расследовании преступлений в сфере информационных технологий.

4. Организация и тактические особенности допроса подозреваемого (обвиняемого) в преступлении в сфере информационных технологий.

5. Допрос свидетелей и потерпевших, проходящих по делу о преступлении в сфере информационных технологий.

6. Тактические и процессуальные особенности производства обыска при расследовании преступлений в сфере информационных технологий.

7. Организация деятельности следователя по проведению обыска при раскрытии уголовных дел в сфере компьютерной информации. Особенности производства обыска в жилище и служебном помещении.

8. Тактика выемки документов и предметов при расследовании уголовных дел о преступлениях в сфере информационных технологий.

9. Особенности производства выемки почтово-телеграфной корреспонденции при расследовании уголовных дел о преступлениях в сфере информационных технологий.

10. Действия следователя на заключительном этапе расследования уголовного дела по преступлению в сфере информационных технологий.

11. Действия следователя по установлению и устранению причин и условий, способствующих совершению преступлений в сфере информационных технологий.

12. Понятие и виды криминалистических учетов. Их использование в раскрытии и расследовании преступлений в сфере информационных технологий.

13. Применение специальных знаний в деятельности органов следствия и дознания при расследовании преступлений в сфере информационных технологий.

14. Понятие, виды образцов для сравнительного исследования и их изъятие при расследовании преступлений в сфере информационных технологий.

15. Понятие, виды и задачи судебных экспертиз, проводимых при расследовании преступлений в сфере информационных технологий.

16. Особенности назначения повторных, дополнительных и комплексных экспертиз при расследовании преступлений в сфере информационных технологий.

17. Анализ, оценка и использование выводов эксперта при расследовании преступлений в сфере информационных технологий.

ЗАКЛЮЧЕНИЕ

Заканчивая исследование в рамках учебного пособия, необходимо выделить следующее положения, рекомендации и выводы.

1. Криминалистическая характеристика преступлений в сфере информационных технологий представляет собой систему взаимозависимых, взаимообусловленных элементов, позволяющих планомерно организовать расследование. Проблемным элементом можно назвать место совершения преступления ввиду неоднозначности его определения. Мы склонны считать, что место нахождения материальных следов (конкретное помещение, где находился компьютер, с которого осуществлялся незаконный доступ), скорее всего, и является местом совершения преступления в сфере информационных технологий. Способы подготовки, совершения и сокрытия следов преступлений в сфере информационных технологий разнообразны, и перечень их видов растет в прямой зависимости от развития информационных технологий.

2. Совершение преступлений в сфере информационных технологий предполагает образование как материальных, так и идеальных следов. Специфика образования, обработки и хранения компьютерной информации предусматривает использование компьютерно-технических средств, на которых (их носителях) возможно материально фиксированное отображение компьютерной информации. Ведется дискуссия в этой связи по вопросу выделения в отдельную группу виртуальных следов, способных сочетать в себе признаки материальных и идеальных следов одновременно, занимая промежуточное положение.

3. В основе совершения преступлений в сфере информационных технологий лежит использование субъектом преступления специальных познаний в этой области. Таким образом, органам, производящим расследование, необходимо осуществлять активную подготовительную работу и анализ, глубоко затрагивающие техническую сторону преступления, особенности функционирования средств и методов, используемых для его совершения, механизм следообразования; консультироваться со специалистами в области информационных технологий.

4. Способы совершения преступлений в сфере информационных технологий (компьютерной информации) коррелируют с видами данного преступления, которые можно сгруппировать следующим образом:

1) непосредственный доступ к электронным носителям и средствам компьютерной техники, содержащим в своей памяти охраняемую законом информацию;

2) дистанционный (удаленный, администрированный) доступ к электронным носителям и охраняемой законом компьютерной информации;

3) фальсификация входных (выходных) данных и управляющих команд;

4) несанкционированное внесение изменений в существующие компьютерные программы и создание вредоносных программных средств;

5) незаконное распространение электронных носителей, содержащих компьютерную информацию;

6) комплексные способы.

5. В результате анализа следственной и судебной практики можно выделить самые распространенные способы совершения мошенничества в сфере компьютерной информации на территории нашего государства:

1) незаконное завладение регистрационными сведениями из разных учетных записей с последующим их применением, например, в мошеннических схемах;

2) использование платежных сервисов разных интернет-ресурсов во время осуществления иным лицом платежных операций для последующего обналичивания чужих денежных средств или приобретения товаров безналичным путем за счет чужих средств;

3) размещение ложных сведений для введения в заблуждение на специально созданном сайте о возможностях получения крупной прибыли от краткосрочных вкладов с последующим заключением виртуальных сделок и переводом денежных средств на счет иностранного банка;

4) взлом электронного кошелька с целью хищения денежных средств путем их обналичивания, перевода на другие счета, оплаты услуг либо товаров через электронные платежные системы типа Qiwi, PayPal, Yandex Money, WebMoney;

5) рассылка на электронную почту спама с вложениями (ссылкой, вставленной в сообщение), содержащими вредоносные программы;

6) рассылка писем-«оферт» об инвестировании бизнеса путем пополнения счета. В случае согласия требуется предоставить персональные данные (например, для юридического лица: образцы подписей, банковские реквизиты и др.);

7) проведение интернет-аукционов и электронных торгов с заведомо несуществующими лотами, где для завышения цены товара мошенники сами делают ставки;

8) создание сайтов-двойников известных интернет-магазинов с целью продажи несуществующих товаров;

9) проведение «благотворительных» акций в Интернете, предлагающих перечислять деньги на счета якобы нуждающихся лиц (тяжело больных, инвалидов и т. п.) либо их родственников. Также могут создаваться сайты-двойники реальных благотворительных организаций;

10) хищение номеров платежных карт посредством специального программного обеспечения или с сайтов-двойников, а также путем физического завладения мобильным телефоном, где подключена услуга «Мобильный банк».

6. Способы совершения мошенничества в сети Интернет коррелируют с видами данного преступления, которые можно сгруппировать следующим образом:

1) мошенничество в Интернете, совершаемое с использованием средств обмена электронными сообщениями (по электронной почте, через социальные сети, с помощью программ-мессенджеров);

2) мошенничество в Интернете посредством использования специально созданных сайтов.

Рассылаемые сообщения можно условно разделить на два вида: сообщения с целью сбора личных данных о потенциальных жертвах преступления; сообщения, в которых содержится предложение совершить денежных перевод на банковскую карту либо сообщить данные банковской карты.

7. С позиций ситуационного подхода первоначальный этап расследования преступлений в сфере компьютерной информации может быть охарактеризован тремя типичными следственными ситуациями, классифицируемыми по субъекту выявления преступления:

1) собственник компьютерной информации обнаружил факт преступления и самостоятельно установил преступника;

2) собственник компьютерной информации обнаружил факт преступления, но преступник остается неустановленным;

3) преступление выявлено правоохранительными органами.

На основе совокупности криминалистически значимых данных, характерных для соответствующих ситуаций, можно выдвигать типичные следственные версии:

1) заявление о преступлении в сфере компьютерной информации подтверждается, преступление действительно имеет место;

2) заявитель ошибается или заблуждается: преступления в сфере компьютерной информации не было, а совершено другое преступление;

3) имеет место ложное заявление о преступлении в сфере компьютерной информации.

8. На этапе возбуждения уголовных дел о преступлениях в сфере компьютерной информации немалую роль играет проведение такого оперативно-разыскного мероприятия, как снятие информации с технических каналов связи. Процесс его организации связан с некоторыми сложностями, в частности с трудностями вычленения из общей массы полученных сведений тех сообщений, которые имеют отношение к предполагаемым действиям преступника.

9. Изъятие носителей информации производится с соблюдением правил, гарантирующих сохранность информации. Перед изъятием устройство необходимо обесточить и упаковать, но в некоторых случаях (например, при сетевых киберпреступлениях, когда на момент осмотра и изъятия устройство включено) перед обесточиванием и изъятием необходимо провести осмотр и зафиксировать все запущенные процессы (исполняемые программы, открытые веб-страницы и документы), либо описав их, либо произведя фото-, видеосъемку экранов с запущенными приложениями и экранов сетевых настроек. При изъятии объектов следует обращать внимание на наличие каких-либо записей на бумаге: многие злоумышленники прячут информацию, используя средства криптографической защиты.

10. В процессе допроса лица, подозреваемого в совершении преступления в сфере информационных технологий, следует принимать во внимание следующие моменты. На эффективность допроса во многом влияет то, в каком психологическом состоянии пребывает допрашиваемый, осознает ли вину, а также имеет ли намерение дать правдивые показания. Следователю необходимо корректно комбинировать и использовать тактические приемы ведения допроса в

целях снижения или нейтрализации негативного психологического состояния и усиления и поддержки позитивного. В ходе подготовки к допросу подозреваемого в совершении преступления, при наличии реальной возможности, следователю стоит получить рекомендацию от психолога в целях выработки наиболее эффективной тактики допроса. Помимо этого, рекомендуется консультация специалиста в области высоких технологий, результаты которой дадут возможность принять во внимание характерные особенности конкретного преступления в рассматриваемой области.

11. Специальные знания с позиции расследования преступлений в сфере компьютерной информации представляют собой углубленные систематизированные знания в области информационных технологий и компьютерной техники, доступные относительно узкому кругу профессионалов, а также навыки практического использования данных знаний, сформированные в ходе профессиональной деятельности.

12. В процессе компьютерно-технической экспертизы компьютера или другого устройства подозреваемого или обвиняемого в совершении преступления в области компьютерной информации, в зависимости от определенного вида компьютерно-технической экспертизы, анализируются следующие объекты: аппаратные объекты (компьютеры, комплектующие для компьютеров и других устройств); периферические устройства (принтеры, сканеры, модемы и т. д.); сетевые аппаратные средства (серверы, сетевые кабели и т. д.); интегрированные системы (мобильные телефоны, органайзеры и др.); программные объекты (системное программное обеспечение, прикладное программное обеспечение); информационные объекты, данные (документы, изготовленные посредством компьютерных средств; данные в мультимедийные форматах (аудио- и видеофайлы, изображения и т. д.).

Список использованных источников

Нормативные правовые акты

1. Конвенция о преступности в сфере компьютерной информации (ETS № 185): заключена в Будапеште 23.11.2001. Доступ из информ.-правовой системы «Гарант».

2. Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18.12.2001 № 174-ФЗ: ред. от 06.03.2019. Доступ из справ.-правовой системы «КонсультантПлюс».

3. Уголовный кодекс Российской Федерации: федер. закон от 13.06.1996 № 63-ФЗ: ред. от 27.12.2018. Доступ из справ.-правовой системы «КонсультантПлюс».

4. О Центральном банке Российской Федерации (Банке России): федер. закон от 10.07.2002 № 86-ФЗ: ред. от 27.12.2018. Доступ из справ.-правовой системы «КонсультантПлюс».

5. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ: ред. от 18.03.2019. Доступ из справ.-правовой системы «КонсультантПлюс».

6. Об оперативно-розыскной деятельности: федер. закон от 12.08.1995 № 144-ФЗ: ред. от 06.07.2016. Доступ из справ.-правовой системы «КонсультантПлюс».

Судебная практика и официальные данные

7. Приговор Ивановского районного суда Амурской области от 12.02.2017 по обвинению Попова Е.В. // Архив Ивановского районного суда Амурской области за 2017 год. Уголовное дело № 1-33/2017.

8. Приговор Кировского районного суда г. Хабаровска от 23.03.2017 по обвинению П. Уголовное дело № 1-3/2017 [Электронный ресурс] // Судебные и нормативные акты РФ: [сайт]. URL: sudact.ru/regular/doc/oHngqimjPHmz (дата обращения: 15.09.2018).

9. Приговор Краснофлотского районного суда г. Хабаровска от 28.07.2017 по обвинению Б. Уголовное дело № 1-174/2017 [Электронный ресурс] // Судебные и нормативные акты РФ: [сайт]. URL: http://sudact.ru/regular/doc/CeseJQvCuuC (дата обращения: 01.05.2018).

10. Приговор Собинского городского суда Владимирской области от 14.12.2017 по обвинению К. Уголовное дело № 1-1-276/2017 [Электронный ресурс] // Судебные и нормативные акты РФ: [сайт]. URL: https://rospravosudie.com/court-sobinskij-gorodskoj-sud-vladimirskaya-oblast-s/act-571745169/ (дата обращения: 06.02.2017).

11. Состояние преступности. Январь 2015 г. – декабрь 2018 г. [Электронный ресурс] // Министерство внутренних дел Российской Федерации: [сайт]. URL: https://мвд.рф/upload/site1/document_news/009/338/947/sb_1612.pdf (дата обращения: 10.03.2019).

12. Агафонов В. В. Особенности формирования доказательств с использованием информации о соединениях между абонентами и (или) абонентскими устройствами: криминалистические и процессуальные аспекты: моногр. М., 2015. 184 с.

13. Батурин Ю. М. Право и политика в компьютерном круге. М., 1987. 112 с.

14. Белкин Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М., 2001. 240 с.

15. Белкин Р. С. Криминалистическая энциклопедия. 2-е изд., доп. М., 2000. 334 с.

16. Брылев В. И., Введенская О. Ю., Пахомов С. В. Интернет-преступления в России: особенности выявления и расследования на первоначальном этапе: учеб. пособие. Краснодар: Краснодар. ун-т МВД России, 2016. 52 с.

17. Вехов В. Б. Особенности расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов: моногр. Волгоград, 2005. 280 с.

18. Вехов В. Б., Голубев В. А. Расследование компьютерных преступлений в странах СНГ. Волгоград, 2004. 304 с.

19. Вехов В. Б., Ковалев С. А. Компьютерное моделирование при расследовании преступлений в сфере компьютерной информации. Волгоград, 2015. 186 с.

20. Вехов В. Б., Попова В. В., Илюшин Д. А. Тактические особенности расследования преступлений в сфере компьютерной информации. М., 2004. 157 с.

21. Возгрин И. А. Введение в криминалистику: история, основы теории, библиография. СПб., 2003. 475 с.

22. Гаврилин Ю. В., Головин А. Ю., Тишутина И. В. Криминалистика в понятиях и терминах: учеб. пособие. М., 2006. 384 с.

23. Грибунов О. П., Старичков М. В. Расследование преступлений в сфере компьютерной информации и высоких технологий: учебное пособие. М., 2017. 160 с.

24. Жердев П. А., Шаров Ю. В. Методы и способы получения доказательственной информации с электронных носителей: курс лекций. Хабаровск: ДВЮИ МВД России, 2013. 100 с.

25. Захарцев С. И. Теория и правовая регламентация оперативно-розыскных мероприятий: дис. ... д-ра юрид. наук. СПб., 2004. 397 с.

26. Захарцев С. И., Игнащенков Ю. Ю., Сальников В. П. Оперативно-розыскная деятельность в XXI веке. М., 2015. 400 с.

27. Зубаха В. С. Общие положения по назначению и производству компьютерно-технической экспертизы. М., 2001. 72 с.

28. Ищенко Е. П. Двуликий электронный янус. М., 2011. 256 с.

29. Колмыков В. В. Преступления в сфере компьютерной информации: науч.-аналит. обзор. Хабаровск, 2006. 48 с.

30. Коломинов В. В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: автореф. дис. … канд. юрид. наук. Иркутск, 2017. 25 с.

31. Крылов В. В. Основы криминалистической теории расследования преступлений в сфере информации: дис. ... д-ра юрид. наук. М., 1998. 334 с.

32. Курс криминалистики. Криминалистическая методика / под ред. О. Н. Коршуновой, А. А. Степанова. СПб., 2004. В 3 т. Т. 3. 571 с.

33. Маевский С. С. Тактика проведения отдельных следственных действий с участием защитника с учетом складывающихся следственных ситуаций: автореф. дис. ... канд. юрид. наук. М., 2010. 32 с.

34. Маркин В. А. Типовые алгоритмы действий при проведении проверки по заявлениям (обращениям) граждан, а также расследовании уголовных дел по преступлениям, совершенным в сфере (с использованием) информационных технологий и сети Интернет: метод. рекомендации. Хабаровск, 2015. 27 с.

35. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. … канд. юрид. наук. Воронеж, 2001. 39 с.

36. Мещеряков Р. В., Шелупанов А. А. Концептуальные вопросы информационной безопасности региона и подготовки кадров. Томск, 2014. 159 с.

37. Ожегов С. И. Словарь русского языка / под ред. Н. Ю. Шведовой. 14-е изд., стер. М., 1983. 944 с.

38. Организационно-тактические аспекты назначения экспертиз, выполняемых в государственных судебно-экспертных учреждениях: учеб. пособие / под ред. А. В. Кузнецова. М., 2019. 134 с.

39. Преступления в сфере компьютерной информации: квалификация и доказывание: учеб. пособие / Ю. В. Гаврилин, А. Ю. Головин, А. В. Кузнецов, Т. В. Толстухина; под ред. Ю. В. Гаврилина. М., 2003. 245 с.

40. Расследование неправомерного доступа к компьютерной информации / под ред. Н. Г. Шурухнова. М., 1999. 254 с.

41. Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. М., 2001. 414 с.

42. Цыкора А. А. Тактико-криминалистические особенности производства следственных действий, связанных с получением и исследованием информации, передаваемой по техническим каналам связи: дис. ... канд. юрид. наук. Ростов-н/Д, 2013. 221 с.

43. Шаталов А. С. Проблемы алгоритмизации расследования преступлений: автореф. дис. ... д-ра юрид. наук. М., 2000. 36 с.

44. Шуклин А. Е. Особенности принятия информационных и тактических решений в сложных следственных ситуациях: автореф. дис. ... канд. юрид. наук. Екатеринбург, 2012. 26 с.

45. Яблоков Н. В. Криминалистика. М., 2017. 239 с.

Статьи в научных изданиях

46. Ахтырская Н. Н. Типичные следственные ситуации и экспертные пути их разрешения // Информационные технологии и безопасность: сб. науч. тр. М., 2017. Вып. 3. С. 133–139.

47. Вараксин В. И., Смирнова С. А. Взаимодействие в судебно-экспертной сфере как условие эффективного противодействия современной преступности // Вестн. криминалистики. 2005. Вып. 2 (14). С. 78–83.

48. Васюков В. Ф. Вопросы назначения и производства экспертиз с использованием информационных технологий // Право и образование. 2019. № 6. С. 100–105.

49. Васюков В. Ф., Булыжкин А. В. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения // Рос. следователь. 2016. № 6. С. 3–8.

50. Васюков В. Ф., Клевцов В. В. Проблемные аспекты привлечения специалиста к процедуре изъятия электронных носителей информации при расследовании распространения «дизайнерских» наркотиков // Преступность в сфере информационно-телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений: сб. материалов всерос. науч.-практ. конф / Воронеж. ин-т МВД России. Воронеж, 2015. С. 80–84.

51. Васюков В. Ф. Некоторые вопросы получения компьютерной информации при осуществлении оперативно-разыскной деятельности // Оперативник (сыщик). 2018. № 2 (55). С. 20–23.

52. Введенская О. Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юрид. наука и правоохран. практика. 2015. № 4 (34). С. 210–214.

53. Вехов В. Б. Особенности расследования DDoS-атак, совершенных на web-серверы организаций // Проблемы борьбы с преступностью: российский и международный опыт: сб. науч. тр. Волгоград, 2016. Вып. 1. С. 25–34.

54. Вехов В. Б. Преступления, связанные с неправомерным использованием баз данных и содержащийся в них компьютерной информации // Защита информации. 2008. № 2. С. 78–81.

55. Воробец И. Н. Глобальная сеть Интернет как пространство для совершения преступлений // Экономические, правовые и прикладные аспекты преодоления кризиса в европейских странах и России: доклады междунар. науч.-практ. конф. / под ред. А. М. Кустова, Т. Ю. Прокофьевой. М., 2012. С. 71–74.

56. Гаврилин Ю. В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Рос. следователь. 2013. № 23. С. 2–6.

57. Дадалко В. А., Протасов К. А. Общая экономическая классификация организованной преступности // Безопасность бизнеса. 2015. № 2. С. 31–37.

58. Дремлюга Р. И. Компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ // Уголов. право. 2018. № 4. С. 52–57.

59. Жердев П. А. Некоторые особенности расследования мошенничества в сфере компьютерной информации // Теория и практика противодействия преступности в Азиатско-Тихоокеанском регионе: сб. материалов междунар. науч.-практ. конф. Хабаровск, 2016. С. 79–85.

60. Киселев Е. А., Смехнов В. А. К вопросу о тактике изъятия доказательств на электронных носителях // Проблемы борьбы с преступностью на современном этапе: сб. материалов всерос. науч.-практ. конф. Хабаровск, 2013. С. 207–212.

61. Колоколов Н. А. Преступления против собственности: комментируем новеллы УК РФ // Мировой судья. 2013. № 1. С. 6–15.

62. Коломинов В. В. О способе совершения мошенничества в сфере компьютерной информации // Человек: преступление и наказание. 2015. № 3. С. 145–149.

63. Коломинов В. В., Смирнова И. Г. К вопросу о формировании криминалистического знания о мошенничестве в сфере компьютерной информации // Уголовно-процессуальные и криминалистические средства обеспечения эффективности уголовного судопроизводства: материалы науч.-практ. конф. Иркутск, 2014. С. 283–289.

64. Комиссаров В. И. Назначение компьютерно-технических экспертиз // Законность. 2000. № 3. С. 31–33.

65. Коновалова А. Б. К вопросу о тактико-процессуальных основах установления следов преступления в высокотехнологичной сфере // Наука и образование: тенденции и перспективы. 2016. № 1 (3). С. 113–116.

66. Корноухов В. Е. Адаптация типовой методики к условиям расследования конкретного преступления // Уголовно-процессуальные и криминалистические чтения на Алтае: материалы науч.-практ. конф. Барнаул, 2013. Вып. 7–8. С. 172–178.

67. Малинин В. Б., Парфенов А. Ф. Способ совершения преступления // Тр. Санкт-Петерб. юрид. ин-та Ген. прокуратуры Рос. Федерации. 2004. № 6. С. 90–94.

68. Мерецкий Н. Е., Жердев П. А. Некоторые особенности хищений денежных средств со счетов граждан при использовании услуги «Мобильный банк» // Вестн. Дальневост. юрид. ин-та МВД России. 2017. № 3. С. 140–146.

69. Мерецкий Н. Е., Шурухнов Н. Г., Жердев П. А. Роль криминалистических данных о механизме функционирования криптовалюты в выявлении и раскрытии преступлений // Вестн. Дальневост. юрид. ин-та МВД России. 2019. № 1. С. 90–96.

70. Мочагин П. В. Новые формы следообразований в криминалистике и судебной экспертизе // Судебная экспертиза в парадигме российской науки: (к 85-летию Ю. Г. Корухова): сб. материалов 54-х криминал. чтений: в 2 ч. М.: Акад. управления МВД России, 2013. Ч. 2. С. 98–102.

71. Мошкин С. В. Типичные следственные ситуации на первоначальном этапе расследования преступлений в сфере компьютерной информации // Ретроспективы и перспективы права. 2013. № 5. С. 48–50.

72. Паненков А. А. Система преступлений в сфере компьютерной информации, входящих в структуру террористической деятельности (кибертерроризм) как реальная угроза внешнему и внутреннему контурам национальной безопасности России // Военно-юрид. журн. 2014. № 3. С. 3–13.

73. Персичкина Н. В. Основные направления использования компьютерных технологий в судебной экспертизе // Проблемы правоведения: сб. науч. статей. Калининград, 2005. С. 104–111.

74. Поляков В. В. Анализ факторов, затрудняющих расследование неправомерного удаленного доступа к компьютерной информации // Проблемы

правовой и технической защиты информации: сб. науч. ст. Барнаул, 2016. С. 17–24.

75. Поляков В. В. Следственные ситуации по делам о неправомерном удаленном доступе к компьютерной информации // Докл. Томского гос. ун-та систем управления и радиоэлектроники. 2010. № 1 (21). С. 46–50.

76. Потапов С. А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации // Социально-экономические явления и процессы. 2016. Т. 11, № 10. С. 90–96.

77. Смирнова И. Г., Коломинов В. В. Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации // Изв. Иркут. гос. экономич. акад. 2015. Т. 6, № 3. С. 27–32.

78. Смушкин А. Б. Виртуальные следы в криминалистике // Законность. 2012. № 8. С. 43–45.

79. Шурухнов Н. Г. Использование при допросе ранее данных объяснений // Тактические приемы допроса и пределы их использования: сб. тез. теорет. семинара, 14 марта 1980 г. М.: ВНИИ МВД СССР, 1980. С. 50–53.

80. Ярцева А. В. Тактика использования информации, полученной с технических каналов связи, в конфликтной следственной ситуации // Закон и право. 2012. № 7. С. 82–86.

Учебное издание

Жердев Павел Александрович, канд. юрид. наук

Расследование преступлений в сфере информационных технологий

Учебное пособие

Редактор *И. В. Кравцова*

Подписано в печать 25.06.2019.
Формат 60 × 84 1/16. Усл. печ. л. 4,4. Тираж 100 экз. Заказ № 7.
Дальневосточный юридический институт МВД России.
Редакционно-издательский отдел. Типография.
680020, г. Хабаровск, пер. Казарменный, 15.