Научная статья
УДК 343.985
https://doi.org/10.36511/2078-5356-2023-4-121-125

Некоторые тактические проблемы выявления и оценки цифровых следов компьютерных преступлений

Лубин Александр Федорович[1], Лубин Сергей Александрович[2]
[1]Нижегородская академия МВД России, Нижний Новгород, Россия, Ale-lubin@yandex.ru
[2]Национальный исследовательский Нижегородский государственный университет имени Н. И. Лобачевского, Нижний Новгород, Россия, Lubin.s@yandex.ru

Аннотация. В статье рассматриваются понятия «цифровой криминалистики», различные мнения авторов, рассматривающие вопросы, связанные с цифровыми следами, а также их оценки при использовании в доказывании. Также предложены некоторые рекомендации следователям по поиску цифровых следов, тактике производства следственных действий при расследовании преступлений в сфере *IT*-технологий и об ошибках доказывания. Сформулированы некоторые предложения о закреплении на законодательном уровне положений о хранении компьютерной информации. В качестве выводов приведены вопросы, характеризующие процесс доказывания при расследовании компьютерных преступлений.

Ключевые слова: цифровые доказательства, собирание цифровых данных, компьютерные преступления, расследование преступлений, следственные действия, уголовный процесс, фиксация цифровых данных, удаленные серверы, электронные носители информации

Для цитирования: Лубин А. Ф., Лубин С. А. Некоторые тактические проблемы выявления и оценки цифровых следов компьютерных преступлений // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. № 4 (64). С. 121–125. https://doi.org/10.36511/2078-5356-2023-4-121-125.

Original article

Some tactical problems of identifying and evaluating digital traces of computer crimes

Alexander F. Lubin[1], Sergey A. Lubin[2]
[1]Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, Nizhny Novgorod, Russian Federation, Ale-lubin@yandex.ru
[2]National Research Lobachevsky State University of Nizhny Novgorod, Nizhny Novgorod, Russian Federation, Lubin.s@yandex.ru

Abstract. The article discusses the concepts of “digital forensics”, various opinions of the authors considering issues related to digital traces, as well as their assessments when used in evidence. Some recommendations are also offered to investigators on the search for digital traces, tactics of investigative actions in the investigation of crimes in the field of IT technologies and on errors of proof. Some proposals have been formulated to consolidate the provisions on the storage of computer information at the legislative level. As conclusions, the questions characterizing the process of proof in the investigation of computer crimes are given.

Keywords: digital evidence, digital data collection, computer crimes, crime investigation, investigative actions, criminal proceedings, digital data fixation, remote servers, electronic media

For citation: Lubin A. F., Lubin S. A. Some tactical problems of identification and evaluation of digital traces of computer crimes. *Legal Science and Practice: Journal of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2023, no. 4 (64), pp. 121–125. (In Russ.). https://doi.org/10.36511/2078-5356-2023-4-121-125.

Строго говоря, «компьютерные преступления» — условное обозначение преступной деятельности, в которой для поиска источников неправомерных доходов, их присвоения и потребления используются любые девайсы, гаджеты, портативные и стационарные компьютеры, маршрутизаторы, переключатели и другие виды сетевых устройств, в том числе и критические серверы, которые позволяют цифровой информации перемещаться независимо от расстояния, от точки отправки к точке ее получения.

С таким же успехом можно говорить об «огнестрельных преступлениях», «взрыво-технических», «ядо-химических» и т. д. Сами по себе средства и способы преступлений не дают оснований объявлять о появлении «цифровой криминалистики», «банковской», «экономической» и пр. Вопрос не в средствах, а в том, что криминалистическая тактика выявления, фиксации, изъятия, оценки и использования следовой картины в доказывании по уголовному делу весьма специфична. Об этом свидетельствуют статистические данные: уровень латентности компьютерных преступлений определяется в настоящее время в 90 %. А из оставшихся 10 % выявленных компьютерных преступлений раскрывается только 1 %. Получается, что у преступников появились новые средства и благоприятные возможности совершения преступлений, а у правоохранительных органов — дефицит тактико-криминалистических рекомендаций по их раскрытию.

Криминалистическая тактика в нашей концепции означает маневрирование наличными средствами в конкретной ситуации. Наличные средства расследования делятся на три группы: 1) информационные средства; 2) процедурные; 3) технико-криминалистические.

Главным информационным средством расследования выступает криминалистическая характеристика компьютерных преступлений, пригодная для выявления, фиксации и оценки «цифровых следов», например, мошенничества в сфере компьютерной информации. Это — необходимая основа для формирования и реализации методики расследования преступлений данного вида. Сказать — легко, но создать такую информационную основу весьма затруднительно.

Во-первых, непонятно, какое звено-элемент является ведущим в типовой версионной цепочке названной характеристики. Если таким элементом выбрать «субъект преступления», то здесь явный дефицит поисковых признаков. Если, например, выбрать на эту роль сетевого администратора, то он, как правило, не судим, не наркоман, практически не имеет связей с криминальной средой. Его действия при передаче конфиденциальной информации между сервером и браузером по протоколу *TCP / IP*, по сути, не видимы. Сетевой администратор жестко не связан с излюбленным способом преступления, о котором могут знать сослуживцы (возможные соучастники). Он много работает («первым приходит, последним уходит»), на хорошем счету у руководства. Он — не тот субъект, «зацепившись» за которого можно легко прочитать следовую картину события преступления. И все же этот субъект может проявлять себя через характерные и видимые следы некоторых действий: а) явное и умышленное искажение входных цифровых данных; б) сокрытие или уничтожение важной входной информации; в) автоматизированная оплата фиктивных услуг и работ, переводы, платежи за не имевшие место покупки, формирование ложного курса на бирже и т. д.

Во-вторых, очевидно, что при расследовании «цифровых» преступлений доминирует не тактика розыска подозреваемых и обвиняемых, а тактика розыска следов их преступной деятельности. Однако именно этих практических алгоритмов для выявления следов и сбора доказательств, применительно к различным ситуациям и способам действий преступников, и не хватает. Имеются в виду случаи ввода личных данных; удаления информации без возможности ее восстановления; внедрения в работу компьютеров дополнительных устройств для ввода и вывода зашифрованной информации; изменения учетной политики; изменения данных, которые находятся на устройстве, ручными исправлениями; внедрения вирусных программ и т. д.

В-третьих, не сформированы тактико-криминалистические рекомендации по анализу, оценке и формам нейтрализации видов противодействия поиску, выявлению и использованию «цифровых следов» в доказывании по соответствующим уголовным делам. Разумеется, путь к «цифровым следам» зачастую лежит через бухгалтерские, управленческие и иные документы, а также через черновые записи и электронную переписку. В такой ситуации совершенно недостаточно помощи простых «компьютерщиков», так как они не обладают «правовыми» знаниями и не способны искать «нужные» (релевантные, относимые), «качественные», «корректные» доказательства. К тому же стоит различать специалистов, которые просто работают с электронными данными в «статике», и лиц, способных

на поиск и фиксацию информационно-телекоммуникационных данных в определенный временной период.

В-четвертых, так или иначе нужны специальные человеческие и технические ресурсы и 100-процентное их включение в процесс расследования. В данном случае представляется целесообразным вариант создания (штатно и технически) Судебно-экспертного центра Следственного комитета Российской Федерации (далее — Центр). Функции этого Центра понятны: участие специалистов Центра в проведении оперативно-розыскных мероприятий по выявлению и фиксации цифровой, доказательственной информации; участие специалистов в производстве следственных действий, направленных на раскрытие компьютерных преступлений и доказывание по уголовным делам о преступлениях данного вида; проведение исследований по оперативным материалам и представление справок специалиста, имеющих, как правило, доказательственное значение; производство судебных экспертиз как средств проверки версий и получения доказательств.

Теперь о том, что касается процедурных ресурсов тактики работы с «цифровыми следами».

На наш взгляд, наивны призывы, чтобы следователь обладал навыками и умениями выполнять специфические процедуры [2]:

а) восстановление данных на машинном носителе, которые были удалены или изменены;

б) расшифровка зашифрованных данных;

в) деактивация систем безопасности (пароли, электронные ключи).

г) установление путей доступа к защищаемой информации и возможных способов ее раскрытия и др.

По нашему мнению, для следователя вполне достаточно производить процедуры, связанные:

1) с правильной организацией взаимодействия с нужными специалистами для осмотра места происшествия, с назначением судебных экспертиз и проведением исследований по оперативным материалам, производством допроса, обыска и выемки — следственных действий, связанных с поиском, фиксацией и изъятием носителей цифровой информации, имеющей доказательственное значение;

2) управлением следственно-оперативной группой на месте происшествия: распределением обязанностей участников осмотра, обменом информацией, фиксацией и изъятием следов, определением количества компьютеров, их расположением в других помещениях, количеством серверов и рабочих станций и режимом их использования, запретом отключения электроснабжения организации путем защиты распределительных щитов; запретом сотрудниками организации выполнять какие-либо операции на компьютерах;

3) полным и корректным составлением текста протокола следственного действия, описанием предметов — вещественных доказательств и любых носителей цифровой информации, а также с их надежной упаковкой и транспортировкой.

Заметим, что, по нашему мнению, участие специалистов в следственных действиях, связанных с поиском и изъятием «цифровых следов», должно стать нормативным, обязательным требованием (по аналогии с ч. 1 ст. 178 УПК РФ «Осмотр трупа. Эксгумация»). Таким же требованием должно быть участие специалиста в оперативно-разыскных мероприятиях.

Быть может, в некоторых простых ситуациях предмет взаимодействия следователя со специалистами-компьютерщиками отсутствует или же он минимален. Например, по уголовному делу Московского городского суда № 2-78\12 по обвинению в статье 105 Уголовного кодекса Российской Федерации в качестве доказательственной базы были исследованы: электронные переписки, интернет-страницы обвиняемых, видеосюжеты с пропагандой националистических идей, записи камер видеонаблюдения [2]. С одной стороны, некоторые следователи такие следы могут самостоятельно и продуктивно воспринять, оценить и тактически верно использовать в доказывании. Однако, с другой стороны, только специалист-компьютерщик способен определить масштаб и ценность следовой («цифровой») картины. В противном случае оправданы «неудобные» вопросы специалиста со стороны защиты прокурору-обвинителю: достаточен ли объем специальных знаний у следователя, чтобы работать с такими специфическими следами? Кроме того, правомерен и другой вопрос защиты: каким образом и в какой форме закреплены выводы следователя? Возможны и такие вопросы: насколько основательны выводы эксперта; насколько апробирована экспертная практика подобных экспертиз и др.

По сути, эти «трудные» вопросы мог бы задать оперативному работнику и следователь, когда он получает результаты оперативно-розыскных мероприятий (далее — ОРМ) при расследовании компьютерных преступлений. Правила, установленные уголовно-процессуаль-

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2023, no. 4 (64)

ным законодательством для закрепления и проверки доказательств, едины для всех сфер деятельности, результаты которых закрепляются и проверяются.

Следует заметить, что законодатель однозначно не говорит о «прямом» использовании результатов ОРМ в качестве доказательств по уголовным делам. Напротив, закреплено предостережение, что, если по каким-то основаниям эти результаты не отвечают необходимым требованиям, то их запрещено использовать в доказывании (ст. 89 УПК РФ). Общепринято, что в «чистом виде», без соответствующих преобразований результаты ОРМ не могут быть доказательствами, даже и в случае известности их источника, законности получения сведений и их достоверности [3, с. 257]. Это означает, что фактические данные должны быть получены:

— субъектами, уполномоченными на проведение соответствующих оперативно-розыскных действий;

— при помощи ОРМ, указанных в статье 6 Закона об ОРД;

— с соблюдением предусмотренного законом и ведомственными нормативными актами порядка ОРМ;

— результаты ОРМ должны быть надлежащим образом зафиксированы в соответствующих оперативно-служебных документах (с последующей систематизацией в деле оперативного учета).

Нам для таких ситуаций представляется актуальными положения о свободе оценки следователем доказательств (ст. 17 УПК РФ), а также нормативные установления о процессуальной самостоятельности следователя (ст. 38 УПК РФ). Следователь вправе по своему усмотрению — решать вопрос, следует ли специально проверять, например, достоверность справок специалистов, которые исследовали носители цифровых доказательств. При этом следователь вправе отстаивать свое решение, понимая свою личную ответственность за его обоснованность и законность. Потому прокурор не вправе указывать следователю пути проверки результатов ОРМ — это прерогатива следователя [4, с. 9].

Заметим, что в качестве существенного недостатка в сфере выявления и использования «цифровых доказательств» следует отметить недопустимые сроки предоставления запрашиваемой информации. Например, операторы сотовой связи по запросу правоохранительных органов представляют информацию в течение нескольких недель или даже месяцев. Заметим, что сроки хранения информации операторами связи ограничены [5–6].

Решить данную проблему можно с помощью изменения законодательства. Например, закрепить возможность получения следователями необходимой информации: 1) о соединениях сотовой связи до возбуждения дела; 2) возможность получения информации сотовой связи в срочном порядке без судебного запроса. Кроме того, информацию предоставлять в структурированном виде и в указанный следователем срок. Наконец, установить более длительное время хранения информации в системах сотовой связи.

Тактическое маневрирование инструментально-техническими средствами съема компьютерной информации — невероятно сложное дело. Оно требует специальной аппаратуры аналоговой и цифровой обработки с применением определенного программного обеспечения и приборов:

— портативных накопителей (выносных винчестеров);

— очень сложных приборов, которые встраиваются в ПК для восстановления информации и сбора данных;

— специализированных программных драйверов;

— интегрированных измерительных оболочек;

— прикладных проблемно-ориентированных пакетов;

— интерактивных проблемно-решающих средств (например, *MathLab*); и др.

В качества общего оптимистичного вывода: новые средства и благоприятные возможности совершения преступлений в эпоху цифровизации, одновременно и закономерно позволяют расширить следовую картину компьютерных преступлений и увеличить диапазон тактических приемов и решений, связанных с выявлением «цифровых» следов, их фиксацией и преобразованием в судебные доказательства.

Список источников

1. Волеводз А. Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. 2002. № 1. С. 4–12.

2. Кассационное определение Верховного суда Российской Федерации от 7 марта 2013 года, дело № 5-013-16СП. URL: https://sudact.ru (дата обращения: 12.04.2023).

3. Маркушин А. Г. Оперативно-разыскная деятельность: учебник и практикум. 5-е изд., перераб. и доп. Москва: Юрайт, 2019.

4. Вартанов А. Р. Проблемы процессуальной самостоятельности следователя по УПК РФ: дис. ... канд. юрид. наук. Краснодар, 2012.

5. Мещеряков В. А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. Воронеж: Воронежский государственный университет, 2001. С. 74–76.

6. О связи: федеральный закон от 7 июля 2003 года № 126-ФЗ // Российская газета. 2003. № 135. 10 июля.

References

1. Vartanov A. R. Problems of procedural independence of an investigator under the Criminal Procedure Code of the Russian Federation. Dissertation... candidate of legal sciences. Krasnodar, 2012. (In Russ.)

2. Volevodz A. G. Traces of crimes committed in computer networks. *Russian investigator*, 2002, no. 1, pp. 4–12. (In Russ.)

3. Cassation ruling of the Supreme Court of the Russian Federation of 7 March 2013 case no. 5-013-16SP. URL: https://sudact.ru (accessed 12.04.2023). (In Russ.)

4. Markushin A. G. Operational investigative activity: textbook and workshop. 5th ed. reprint. and add. Moskow: Yurayt Publ., 2019. (In Russ.)

5. Meshcheryakov V. A. Crimes in the field of computer information: legal and forensic analysis. Voronezh: Voronezh State University Publ, 2001. Pp. 74–76. (In Russ.)

6. On Communications: federal law no. 126-FZ of July 7, 2003. *Rossiyskaya Gazeta,* 2003, no. 135, July 10. (In Russ.)

Информация об авторах

А. Ф. Лубин — доктор юридических наук, профессор;
С. А. Лубин — кандидат юридических наук, доцент.

Information about the authors

A. F. Lubin — Doctor of Science (Law), Professor;
S. A. Lubin — Candidate of Science (Law), Associate Professor.

Статья поступила в редакцию 05.09.2023; одобрена после рецензирования 20.10.2023; принята к публикации 12.12.2023.

The article was submitted 05.09.2023; approved after reviewing 20.10.2023; accepted for publication 12.12.2023.