УДК 343.98
DOI https://doi.org/10.17308/vsu.proc.law.2021.3/3554

ВИДЫ ЦИФРОВОЙ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ, ПОЛУЧАЕМОЙ В ХОДЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

В. Н. Цимбал

Московский университет МВД России имени В. Я. Кикотя

Поступила в редакцию 15 января 2021 г.

Аннотация: *тематикой научной статьи стало изучение цифровой криминалистически значимой информации, которая может оставаться в результате совершения преступлений в сфере компьютерной информации или с использованием информационно-телекоммуникационных технологий. Автором предложено разделение на группы используемых средств совершения преступлений и классификация цифровых следов, получаемых при изучении криминалистически значимой информации. Обозначаются также формы привлечения лиц, обладающих специальными знаниями для работы с обнаруженными следами и перечень судебных экспертиз, которые необходимо проводить для получения доказательственной информации.*

Ключевые слова: *криминалистически значимая информация, следы преступления, цифровой след, информационная сфера, цифровые доказательства, специальные знания, судебная экспертиза.*

Abstract: *the topic of the scientific article was the study of digital criminologically significant information, which may remain because of crimes in the field of computer information or using information and telecommunication technologies. The author proposes: the division into groups of the means used to commit crimes and the classification of digital traces obtained when studying criminologically significant information. They also indicate the forms of involvement of persons with special knowledge to work with discovered traces and the list of forensic examinations that must be carried out to obtain evidence information.*

Key words: *criminally significant information, traces of crime, digital trace, information sphere, digital evidence, special knowledge, forensic examination.*

Пандемия короновируса во всем мире сказалась на жизни людей, их заработках, состоянии бизнеса, доходах государств и, конечно, состоянии преступности.

Согласно опубликованной статистике ГИАЦ МВД России, за 10 месяцев 2020 г. наблюдался рост преступлений в сфере компьютерной информации либо совершенных с использованием информационно-телекоммуникационных технологий. Утверждать однозначно, что это связанно только с вышеуказанной пандемией нельзя, однако исключить, что сложившаяся ситуация оказала на рост такой преступности непосредственное влияние, можно. Так, всего совершенных преступлений в обозначенной сфере более 420 тыс. (рост +75,1 % по сравнению с аналогичным периодом прошлого года, далее – АППГ), из них: мошенничество

с использованием электронных средств платежа (ст. 159.3 УК РФ) – более 24,5 тыс. (+96,2 % в сравнении с АППГ), преступления в сфере компьютерной информации (ст. 272, 273 УК РФ – 3708 (рост на 56,1 %))[1].

По данным Генеральной прокуратуры РФ на ноябрь 2020 г., использовались или применялись злоумышленниками при совершении противоправных деяний: расчетные (пластиковые) карты (в более чем в 174 тыс. зарегистрированных преступлений), компьютерная техника (в 26,6 тыс. преступлений), сеть «Интернет» (более чем в 268 тыс. преступлений), средства мобильной связи (более чем в 197 тыс. преступлений), программных средств (более чем в 8,8 тыс. преступлений), фиктивных электронных платежей (в 1,1 тыс. преступлений)[2].

Как видим, отмечается рост преступлений практически по всем позициям ведущейся статистики. Причины тому различные: распространенность средств информатизации, смещение тренда бизнеса на предоставление дистанционных и цифровых услуг, доступность данных услуг для населения, слабое знание гражданами основ информационной безопасности, активизация преступного элемента (смещение его интересов в информационную сферу) и т. п. Конечно, нельзя исключать и пандемию, бушующую в мире, которая, несомненно, повлияла на рост числа преступлений.

Предметы и способы совершения преступлений в сфере высоких технологий, в информационной сфере, компьютерных преступлений изучали многие ученые, например: Д. В. Бахтеев, В. Б. Вехов, В. Н. Карагодин, И. П. Родивилин, Е. Р. Россинская[3] и др.

Современная преступность, как было отмечено помимо классических средств совершения преступлений (нож, пистолет, лом, взрывчатка и т. п.), всё чаще использует информационные технологии и всевозможные

[1] Состояние преступности в России за январь-октябрь 2020 г. URL: https://мвд.рф/reports/item/21933965 (дата обращения: 24.12.2020).

[2] Состояние преступности в России за январь-ноябрь 2020 г. URL: http://crimestat.ru/analytics (дата обращения: 30.12.2020).

[3] См.: *Бахтеев Д. В.* Криминалистическая классификация цифровой доказательственной информации // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) : сб. статей Междунар. науч.-практ. конф. М., 2018. С. 44–49 ; *Вехов В. Б.* Компьютерные преступления : способы совершения и раскрытия ; под ред. Б. П. Смагоринского. М., 1996 ; *Карагодин В. Н.* Особенности способов преступлений, совершаемых с использованием цифровых технологий // Академическая мысль. 2020. № 2 (11). С. 17–20 ; *Родивилин И. П.* Использование компьютерной информации при раскрытии и расследовании преступлений, совершенных с использованием сети «Интернет» // Криминалистика : вчера, сегодня, завтра : сб. науч. трудов. Иркутск, 2015. Вып. 6. С. 173–178 ; *Россинская Е. Р.* Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 5 (57). С. 31–44 ; *Россинская Е. Р., Сааков Т. А.* Проблемы собирания цифровых следов преступлений из социальных сетей или мессенджеров // Криминалистика : вчера, сегодня, завтра. 2020. № 3 (15). С. 106–123.

решения для реализации своих преступных замыслов: вирусы, компьютеры, серверы, мобильные телефоны, смартфоны, записывающие средства, сеть «Интернет» и т. д.

Все перечисленные средства можно разделить на следующие группы:

1) компьютерная техника (ПЭВМ, периферийное оборудование, планшетные компьютеры и т. п.);

2) специализированное программное обеспечение (вредоносные программы, программы для анализа сетей, программы для подбора паролей и т. п.);

3) средства организации связи и коммуникаций (средства подвижной радиотелефонной связи – мобильные и спутниковые телефоны, смартфоны, радиостанции), серверное оборудование, коммуникационные средства – роутеры, модемы, коммутаторы, сетевые карты) и т. п.;

4) аппаратные средства (генераторы зашумления, средства физического уничтожения информации, скиммеры и т. п.);

5) цифровые технологии (фишинговые сайты, поддельная электронная почта, счета в платежных системах – ЮMoney (ранее Яндекс Деньги), кошелек Qiwi) и т. п.

Безусловно, указанные группы оставляют различные следы, которые будут интересовать следователя. При исследовании объектов, предметов или орудий с мест совершения преступлений они будут нести на/в себе криминалистически значимую информацию, под которой понимаются любые данные (сведения, события, факты) независимо от принимаемой ими формы, получаемые непроцессуальным и (или) процессуальным путем, имеющие справочное, ориентирующее и (или) доказательственное значение и используемые для решения задач уголовного судопроизводства[4].

В контексте рассматриваемой тематики нас интересуют оставляемые цифровые следы, которые, как справедливо отмечает Е. Р. Россинская «…представляют собой криминалистически значимую компьютерную информацию о событиях и действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи»[5]. Такие следы имеют специфические свойства и обладают следующими особенностями: и по форме и/или способу отражения (файлы, базы данных, компьютерные программы), и по свойству такой информации (нематериальные, легко изменяемые, на высоких скоростях перемещаемые в пространстве).

Представляться такие следы могут в виде команд или данных в операционной системе, отдельной компьютерной программы, файлов с текстовой, графической, символьной информацией, баз данных, сообще-

[4] См.: *Цимбал В. Н.* Понятие и научное значение криминалистически значимой информации // Общество и право. 2014. № 4 (50). С. 242.

[5] *Россинская Е. Р.* Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 5 (57). С. 35.

ний электронной почты (мессенджера, чата, форума), сведений о работе устройства, сайтов в сети «Интернет».

Цифровые следы могут оставаться на устройствах преступника, потерпевшего, средствах и системах коммуникации, в данных провайдера, в ресурсах сети «Интернет». Образовываться они могут как в результате деятельности человека, функционирования оборудования, так и в обоих случаях.

Рассмотреть разновидности цифровых следов, получаемых при изучении криминалистически значимой информации, можно по различным основаниям: способу отображения; виду следа; месту нахождения; наличию (отсутствию) семантического значения; возможности идентификации данных; доступности сведений для исследователя.

По способу отображения цифровые следы могут представляться как *статичные* (фотография, стоп-кадр из видеоряда либо скриншот с экрана устройства, изображения в различных форматах, таблицы, рисунка, схемы, диаграммы) и *динамические изображения* (видеозапись, художественное произведение, прямая трансляция с камеры устройства с передачей видеопотока в сеть «Интернет» (так называемый «стрим» либо «лайв-вещание»), изображений с камер наблюдения); *аудиозаписи* (голосовые сообщения в мессенджерах, музыкальные произведения); *текстовый вид* (документы в текстовых редакторах, сообщения в мессенджерах (чатах, форумах, электронной почте)); *символьный вид* (зашифрованные данные, строки программного кода, реестр и/или конфигурационные файлы операционной системы) и *комбинированном виде* (операционная система и/или ее журнал событий, веб-сайт, компьютерная программа).

По виду цифрового следа они могут представляться как *файлы* (различных расширений – «.dbf», «.txt», «.exe», «.c», «.doc», «.sh», «.pdf», «.jpeg», «.tar»); векторные или растровые *изображения*; *наборы файлов*, которые могут включать в себя текст, изображение, графику, ссылки (например, веб-страница).

По месту нахождения можно выделить информацию, отображенную на носителях информации: *многократно перезаписываемых запоминающих устройствах* (жестких дисках, твердотельных накопителях, компакт и блюрей дисках, флеш-картах), *оперативной памяти* или *оперативном запоминающем устройстве*, *магнитных картах* и другом (пластиковых банковских, транспортных и иных видах карт, RFID-метках, магнитных ключах, пропусках), *облачных хранилищах* (Google Диск, Яндекс Диск, Облако Mail.Ru, Dropbox и др.). В последнем случае необходимо пояснить, что фактически носителем информации облачное хранилище не является, так как информация в них хранится на специальных накопителях информации[6]. Получить информацию из облачного хранилища возможно только по запросу, физическое изъятие носителя или снятие образа из него довольно затруднительно, особенно если это зарубежный

[6] Как устроены хранилища данных // Хабр [сайт]. URL: https://habr.com/ru/company/1cloud/blog/345154 (дата обращения: 27.12.2020).

ресурс, где владелец может продолжительное время отвечать или вообще проигнорировать обращение правоохранительных органов.

Следующим основанием является информация, имеющая *семантическое значение,* и рассматривать ее мы будем в двух случаях. В первом речь идет о понимании смысла обнаруженной криминалистически значимой информации человеком, и он может ее интерпретировать сразу (например, текстовый документ, изображение). Во втором случае информация может не нести для человека семантического содержания, однако может легко читаться машиной (например, битовый поток данных, управляющая команда в операционной системе). Для интерпретации подобной информации требуется ее обработка при помощи того же компьютера или программы, с целью дальнейшего получения значимых сведений.

Следующий классификационный признак позволяет *установить и идентифицировать* полученную криминалистически значимую информацию. В этом случае исследование данных должно точно определить, какой процесс оставил тот или иной след, откуда пришла команда либо это промежуточная точка (т. е. устройство потерпевшего использовалось как передаточное звено в цепочке событий преступного деяния), кто выполнил действие – человек, машина, программа либо это совокупность действий. Эти данные позволят достоверно установить причинно-следственную связь случившегося, определить механизм действий.

И последним в нашей классификации будет признак доступности сведений для обнаружения и исследования. Разделить данный признак можно на несколько составляющих: первое – информация *открыта*, т. е. доступна без каких-либо сложных способов ее извлечения, находится «на виду»; второе – информация *скрыта*, т. е. преступник предпринял какие-то действия, направленные на сокрытие следов своей деятельности (уничтожение, использование стеганографических методов, подделка и т. п.), либо сведения необходимо восстанавливать после удаления или применять специальные программные решения для ее нахождения; третье – информация *зашифрована*, т. е. злоумышленниками применяются методы криптографической защиты данных, при сложных алгоритмах которых получить семантическое содержание такой информации практически невозможно.

Конечно, процедуры извлечения, закрепления, анализа и исследования полученной криминалистически значимой цифровой информации требуют привлечения лиц, обладающих специальными знаниями. Их формы следующие: непроцессуальная – консультирование, помощь в изъятии; процессуальная – проведение судебной экспертизы, допрос в качестве специалиста и/или эксперта.

Лицо, производящее расследование для получения доказательственной информации в зависимости от полученной криминалистически значимой информации и произошедшего события может назначить следующие виды судебных экспертиз: автороведческую, бухгалтерскую, видеотехническую, компьютерную, лингвистическую, налоговую, порт-

ретную, радиотехническую, технико-криминалистическую экспертизу документов, фоноскопическую, фототехническую. В отдельных случаях, целесообразно назначить комплекс судебных экспертиз или комплексную судебную экспертизу.

Вывод о том, что эпидемиологическая обстановка в мире и России некоторым образом повлияла на рост преступной деятельности в информационной сфере, можно сделать в связи с наличием некоторых факторов, которые стали подспорьем этому, а именно: продолжительное нахождение людей дома, переход большинства организаций на удаленную работу в период введения режима самоизоляции, в крупных городах с развитой услугой курьерской или иной разновидности доставки товаров (от еды до техники), что позволяет не покидать дома и соответственно использовать для всего этого сеть «Интернет». С начала режима самоизоляции в апреле 2020 г. оборот крупных ретейлеров увеличился почти на 24 % по сравнению с мартом и на 36 % по сравнению с апрелем 2019 г. Онлайн-заказов в целом стало на 25 % больше[7]. В свою очередь, преступный элемент воспользовался данной вынужденной ситуацией и активно совершал преступления, о чем свидетельствуют приведенные цифры.

Таким образом, проблема получения криминалистически значимой информации и ее анализ правоохранительными органами не теряет своей актуальности и из года в год становится только острей, а повсеместная цифровизация и разнообразные форс-мажорные обстоятельства оказывают на это непосредственное влияние.

Библиографический список

Бахтеев Д. В. Криминалистическая классификация цифровой доказательственной информации // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) : сб. статей Междунар. науч.-практ. конф. М. : Академия управления МВД России, 2018. С. 44–49.

Вехов В. Б. Компьютерные преступления : способы совершения и раскрытия / под ред. Б. П. Смагоринского. М. : Право и закон, 1996. 182 с.

Карагодин В. Н. Особенности способов преступлений, совершаемых с использованием цифровых технологий // Академическая мысль. 2020. № 2 (11). С. 17–20.

Родивилин И. П. Использование компьютерной информации при раскрытии и расследовании преступлений, совершенных с использованием сети «Интернет» // Криминалистика : вчера, сегодня, завтра : сб. науч. трудов. Иркутск : Восточно-Сибирский институт МВД России, 2015. Вып. 6. С. 173–178.

Россинская Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 5 (57). С. 31–44.

[7] Что и как покупают в Интернете жители России : аналитика и статистика за 2020 год. URL: https://cms-rating.ru/chto-i-kak-pokupayut-v-internete (дата обращения: 27.12.2020).

Россинская Е. Р., Сааков Т. А. Проблемы собирания цифровых следов преступлений из социальных сетей или мессенджеров // Криминалистика : вчера, сегодня, завтра. 2020. № 3 (15). С. 106–123.

Цимбал В. Н. Понятие и научное значение криминалистически значимой информации // Общество и право. 2014. № 4 (50). С. 239–243.

References

Bahteev D. V. Forensic classification of digital evidence // International scientific-practical conference "Criminalistics in the development of the information society (59th annual forensic reading)" [electronic resource] : The collection at the International scientific-practical conference. M. : Management Academy of the Ministry of the Interior of Russia, 2018. P. 44–49.

Vehov V. B. Computer crimes: methods of commission and disclosure ; edited by B. P. Smagorinskiy. M. : Law and the law, 1996. 182 p.

Karagodin V. N. Features of Ways of Crimes, Committed Through the Use of Digital Technologies // Academic Thought. 2020. № 2 (11). P. 17–20.

Rodivilin I. P. Use of computer information in the disclosure and investigation of Internet crimes // Forensics: Yesterday, Today, Tomorrow : collection of scientific papers. Irkutsk : East-Siberian Institute of the Ministry of Internal Affairs of the Russian Federation, 2015. № 6. P. 173–178.

Rossinskaya E. R. Problems the use of special knowledge for the judicial investigation of computer crimes in the conditions of digitalization // Courier of Kutafin Moscow State Law University (MSAL). 2019. № 5 (57). P. 31–44.

Rossinskaya E. R., Saakov T. A. The problems of collecting digital footprints of crimes in social networks and messengers // Forensics: Yesterday, Today, Tomorrow : collection of scientific papers. Irkutsk : East-Siberian Institute of the Ministry of Internal Affairs of the Russian Federation, 2020. № 3 (15). P. 106–123.

Tsimbal V. N. Concept and scientific importance of forensically important information // Society and Law. 2014. № 4 (50). P. 239–243.

Для цитирования:

Цимбал В. Н. Виды цифровой криминалистически значимой информации, получаемой в ходе расследования преступлений // Вестник Воронежского государственного университета. Серия: Право. 2021. № 3 (46). С. 249–255. DOI: https://doi.org/10.17308/vsu.proc.law.2021.3/3554

Recommended citation:

Tsimbal V. N. Types of digital criminologically relevant information obtained during the investigation of crimes // Proceedings of Voronezh State University. Series: Law. 2021. № 3 (46). P. 249–255. DOI: https://doi.org/10.17308/vsu.proc.law.2021.3/3554

Московский университет МВД России имени В. Я. Кикотя

Цимбал В. Н., кандидат юридических наук, доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий

E-mail: sedruk@mail.ru

Moscow University of the Russian Ministry of Internal Affairs named after V.Ya. Kikot

Tsimbal V. N., Candidate of Legal Sciences, Associate Professor of the Special Information Technologies of the Educational and Scientific Complex of Information Technologies Department

E-mail: sedruk@mail.ru