УДК 343.9

Л. А. Спектор, А. Д. Малютин

Институт сферы обслуживания и предпринимательства (филиал) ДГТУ в г. Шахты, Шахты, e-mail: Spektor2@mail.ru

ЦИФРОВАЯ КРИМИНАЛИСТИКА В УСЛОВИЯХ КОМПЬЮТЕРИЗАЦИИ СОВРЕМЕННОГО ОБЩЕСТВА

Ключевые слова: цифровая криминалистика, компьютеризация, цифровые следы, компьютерные технологии, цифровые преступления.

В данной работе авторами поднимается вопрос необходимости использования и усовершенствования методов цифровой криминалистики при расследовании различного рода компьютерных преступлений. Рассматриваются цели и особенности цифровой криминалистики, а также выделяются специальные оперативно-розыскные мероприятия, которые связаны со спецификой технического оборудования и необходимы при расследовании компьютерных преступлений. Практически каждая наука вырабатывала свое понимание информации и исследовала различные ее формы и аспекты. В XX веке появился новый вид информации – информация, циркулирующая в компьютерах, а впоследствии, и в иных информационно-технологических устройствах. Однако несмотря на то, что с момента появления первого компьютера прошло уже более 7 десятков лет (полагаем, что первым компьютером можно считать британский Colossus, запущенный в 1943 г.), а с теоретического обоснования разработок области компьютеров и компьютерной информации еще больше времени (теорию заложил еще Чарльз Бэббидж в 1830 г.), до сих пор отсутствует даже общепринятый термин, отражающий сущность данной информации, а также универсальный подход к трактовке рассматриваемой категории. Жизнь современного общества сложно представить без использования компьютерной техники, смартфонов, планшетов, а также предоставляемого такими устройствами доступа к виртуальному пространству сети Интернет, социальным сетям, интернет-магазинам, услугам, предоставляемым в дистанционной форме. Однако все преимущества и достоинства эпохи повсеместной цифровизации сопровождаются появлением криминальной деятельности в этой новой среде существования человечества. Это, в свою очередь, вызывает необходимость активного исследования ее специфики и использования получаемых результатов в правоохранительной деятельности. В последнее время уже достаточно прочно оформилось и сложилось в качестве относительно самостоятельного, но органически тесно связанного, основанного и неотделимого от науки криминалистики направление, получившее название цифровой криминалистики.

L. A. Spector, A. D. Malyutin

Institute of Service and Entrepreneurship (branch) of DGTU in Shakhty, Shakhty, e-mail: Shpigunova96@mail.ru

DIGITAL CRIMINALISTICS IN THE CONDITIONS OF COMPUTERIZATION OF MODERN SOCIETY

Keywords: digital forensics, computerization, digital traces, computer technology, digital crimes

In this paper, the authors raise the question of the need to use and improve the methods of digital forensics in the investigation of various kinds of computer crimes. The purposes and features of digital criminalistics are considered, and special operational investigative measures are highlighted, which are related to the specifics of technical equipment and are necessary in the investigation of computer crimes. Almost every science has developed its own understanding of information and explored its various forms and aspects. In the XX century, a new type of information appeared – information circulating in computers, and subsequently in other information technology devices. However, despite the fact that more than 7 decades have passed since the appearance of the first computer (we believe that the British Colossus, launched in 1943, can be considered the first computer), and even more time has passed since the theoretical justification of developments in the field of computers and computer information (the theory was laid by Charles Babbage in 1830), until now there is not even a generally accepted term reflecting the essence of this information, as well as a universal approach to the interpretation of the category in question. It is difficult to imagine the life of modern society without the use of computer technology, smartphones, tablets, as well as access provided by

such devices to the virtual space of the Internet, social networks, online stores, services provided remotely. However, all the advantages and advantages of the era of ubiquitous digitalization are accompanied by the emergence of criminal activity in this new environment of human existence. This, in turn, causes the need for an active study of its specifics and the use of the results obtained in law enforcement. Recently, the direction called digital criminology has already taken shape and developed quite firmly as a relatively independent, but organically closely related, based and inseparable from the science of criminology.

Введение

Судебно-следственная практика свидетельствует об использовании преступниками цифровых технологий и цифровой информации при совершении преступлений. Это относится не только к техническим средствам, используемым для взаимодействия между членами преступной группы, но и к возможности через информационно-телекоммуникационные сети распространять запрещенную законом информацию, например, ст. 207 УК РФ (Заведомо ложное сообщение об акте терроризма), ст.110.1 УК РФ (Склонение к совершению самоубийства или содействие совершению самоубийства), ст. 242.1 УК РФ (Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних) и др. Компьютерно-технические средства широко используются при совершении преступлений в сфере экономики, при незаконном обороте наркотических средств и иных преступлениях. Для достижения криминалистических целей, по нашему мнению, релевантная цифровая информация может использоваться в различных формах, а именно, как справочная, как оперативная (розыскная) и как доказательственная.

Целью данной работы является изучение механизма следообразования в цифровой среде современного кибернетического пространства (информационной инфраструктуры) и особенностями формирования на его основе судебных доказательств.

Материал и методы исследования

Исследование базируется на общенаучном диалектическом методе познания объективной действительности, а также на специальных методах исследования. Обоснованность выводов и рекомендаций, содержащихся в работе, достигается за счет комплексного применения диалектического, аналитического, логического, исторического, системно-структурного, сравнительно-правового, юридико-лингвистического методов.

Результаты исследования и их обсуждение

На сегодняшний день, одним из стратегических направлений реализации государственной политики является научно-технологическое развитие Российской Федерации. Информационно-телекоммуникационные технологии активно внедряются во все сферы жизнедеятельности гражданского общества (социальную, управленческую, здравоохранительную, правоохранительную и т.д.). Вместе с тем, по данным Генеральной прокуратуры Российской Федерации, в 2019 г. отмечался рост преступлений, совершенных с использованием сети Интернет, с 65,9 тысячи (в 2018 г.) до 91,6 тысячи. Следует отметить, что правовое регулирование данной сферы жизнедеятельности общества зачастую не отвечает запросам ее развития. Ярким примером может служить блокчейн-технология, являющаяся системообразующим звеном оборота криптовалюты. Законодательное определение этого платежного документа отсутствует. Вместе с тем возможности ее оборота в виртуальном пространстве неограниченны. Этим обусловлен рост механизмов преступной деятельности в данном направлении, где криптовалюта может являться как средством совершения преступления, так и предметом преступного посягательства. В данном случае следует говорить о формировании компьютерной криминалистики как отрасли знаний, умений и навыков, направленных на формирование компетенций по выявлению, раскрытию и расследованию преступлений в сфере информационно-телекоммуникационных технологий, криминалистическому исследованию электронной доказательственной информации [1, с. 530].

Преступления указанной категории совершаются бесконтактным способом, что значительно сокращает возможность выявления трасологических следов и вместе с тем увеличивает число цифровых следов. Под цифровым следом в данной статье понимается уникальный набор действий, производимый в информационно-телекоммуника-

ционной среде, а также информация, оставленная в результате просмотра веб-страниц. Цифровой след может быть оставлен как физическим, так и юридическим лицом.

Предпосылками возникновения цифровой криминалистики стало:

1. Возникновение и активное развитие кибернетического пространства (информационной инфраструктуры) как новой специфической среды существования и активной деятельности современного человека с принципиально новыми системообразующими элементами. В качестве данных элементов выступают компьютеры, компьютерные сети (в первую очередь сеть Интернет), системы мобильных телекоммуникаций, глобальные навигационные системы, интернет-экономика и т. д.

2. Формирование принципиально новых видов правоотношений, складывающихся вокруг объектов и явлений в кибернетическом пространстве, не имеющих аналогов в традиционном материальном мире. В частности, речь идет об интернет-сайтах, системе доменных имен, компьютерных программах (особенно самовоспроизводящихся, получивших свою известность как компьютерные вирусы), системах распределенных реестров (Blockchain), ставших основой для построения целого спектра криптовалют, социальных сетях, беспилотных транспортных платформах и др.

3. Возникновение новых видов посягательств на складывающиеся правоотношения в кибернетическом пространстве. Например, использование вредоносных программ, зеркалирование и подмена интернет-ресурсов, перехват реальной и генерация фиктивной (намеренно искаженной) информации и т. д.

4. Расширение представления о механизме следообразования за счет дополнения его закономерностями кибернетического пространства, а именно: электронно-цифровое отображение, виртуальные следы, новые свойства возникающих следов, особенности формирования следовой картины и т. д

Правоохранительные органы для криминалистических целей осуществляют накопление, обработку, систематизацию, хранение и выдачу справочной и учетной информации, в том числе цифровой. Так, например, органы полиции ведут видеобанки и видеотеки лиц, проходивших (проходящих) по делам и материалам проверок полиции; формируют, ведут и используют банки данных оперативно- справочной, криминалистической, экспертно- криминалистической, розыскной и иной информации о лицах, предметах и фактах. Также используются разнообразные интеграционные программные обеспечения, позволяющие расширить используемые технические средства. К подобным можно отнести программу распознавания лиц «FindFace». Камеры видеонаблюдения, к которым будет подключена данная программа, смогут в режиме реального времени проводить анализ получаемых изображений и таким образом выявлять правонарушителей [2, с. 231].

Уровень развития цифровых технологий позволяет подходить к реализации таких проектов, как «Умный город». Это комплекс программно – технических решений и организационных мероприятий, направленные на эффективное использование всех видов ресурсов (электричество, вода, газ, тепло, время) и создающие условия для удобного пребывания в городе, комфортного для проживания и ведения бизнеса [3, с. 16]. Подобная компьютеризация города позволяет использовать технологии, так называемые “Приборы разведки”, для сбора и анализа данных о поведении субъекта, маршрутах его перемещения и лицах, с которыми он контактирует. Примером использования подобных приборов может быть Амстердам. Для достижения целей оперативно-розыскной деятельности (ОРД) разработано множество технических средств, позволяющих негласно получать информацию при осуществлении данной деятельности. Перечень специальных технических средств, используемых органами, осуществляющими ОРД, дан в Постановлении Правительства.

Без использования цифровых технологий было бы невозможно получение такой информации, в силу ее специфики. Современная криминалистика должна приспосабливаться, адаптироваться к уровню развития современных технологий для возможности их использования в целях оказания содействия осуществлению правоохранительной деятельности.

В настоящее время часто стал упоминаться термин «Цифровая криминалистика». Это связано, во-первых, с тем, что совершение преступлений с использованием цифровых устройств оставляет в них электронные криминалистически-значимые следы, а во-

вторых, с тем, что органы предварительного расследования имеют технико- криминалистические средства (персональные компьютеры), позволяющие изготавливать процессуальные документы в электронной форме на электронных носителях информации. Это нашло отражение и в нормах УПК РФ. Статьи 164, 189 УПК РФ и другие допускают возможность фиксации следов преступления, хода следственных действий посредством технических средств.

При совершении киберпреступлений часто проводятся прямые атаки на компьютеры и другие подобные устройства с целью их отключения. Иногда атакуемые компьютеры используются для распространения вредоносных программ, нелегальной информации, различного рода изображений (например, детской порнографии) и экстремистских материалов. В новейшей юридической литературе выделяются следующие виды киберпреступлений: корыстные киберпреступления (включая фишинг, кибер-вымогательство, финансовое мошенничество и др.); кража персональных данных; кибершпионаж; киберзапугивание; нарушение авторских прав и некоторые другие. Рассматривая их, следует учитывать, что в современных условиях в легальный экономический оборот активно входят «нетрадиционные» виды собственности, в том числе веб-сайты, криптовалюты, технологии мобильной связи, интернет-собственность и др.

Поскольку они обладают способностью генерировать высокие доходы, криминальная среда реагирует на них соответствующим образом. В результате появляются новые виды преступных посягательств, предполагающие использование современных информационных технологий на основе внезапности и анонимности.

Практически все эти противоправные действия гораздо опаснее преступлений, совершенных за пределами киберпространства, поскольку способны нанести ущерб всем охраняемым законом интересам. Они варьируются от частных неимущественных потребностей отдельных граждан до нужд безопасности государства. Анализ официальной криминальной статистики показывает, что в условиях пандемии коронавируса общий уровень преступности в России остался прежним, однако число киберпреступлений резко возросло. Это не только издержки цифровизации общества, но и результат того, что люди, находясь в самоизоляции, имеют больше возможностей усваивать различные знания онлайн, в том числе криминальной направленности, и применять их на практике.

Такое положение дел привело к тому, что в 2019 году в структуре одного из ключевых управлений Следственного комитета Российской Федерации было создано новое подразделение – Управление по расследованию киберпреступлений и преступлений в сфере высоких технологий. Вскоре после этого аналогичное подразделение по борьбе с ИТ-преступлениями появилось в Следственном департаменте МВД России. Их возникновение связано не только с ярко выраженной специфичностью, массовостью и высокой латентностью киберпреступлений, но и с присущим им межрегиональным и международным характером. Министерство внутренних дел Российской Федерации опубликовало статистику, согласно которой за первые 10 месяцев 2020 года было зарегистрировано 420 700 киберпреступлений (+75%), из которых 216 000 − тяжкие или особо тяжкие (+84%).

Количество преступлений с использованием сети «Интернет» в том же году увеличилось на 93% и составило 243 600 единиц, а с использованием мобильной связи − на 96% и достигло 181 200 единиц. За тот же период рост числа преступлений с использованием банковских карт составил более 480%. Лидером по росту киберпреступности в этот период был Санкт-Петербург, где таких преступных деяний совершено на 290,5% больше, чем в предыдущем году. Немного отстают Калужская область (207,3%), Карачаево-Черкесия (185,1%), Ингушетия (142,1%) и Самарская область (119,9%). Самые низкие темпы их роста наблюдаются в Тыве (32,2%), Адыгее (20%), Смоленской области (11,2%), Северной Осетии−Алании (6,9%) и Кировской области (3,8%). В то же время самый высокий уровень раскрываемости таких преступлений наблюдается в Дагестане. Там эффективность борьбы с киберпреступниками возросла на 65%. Далее идут Карачаево-Черкесия (58,1%), Чечня (58%), Чукотка (53%) и Ингушетия (42,6%). Самый низкий показатель их раскрытия в Башкортостане (16,1%), Краснодарском крае (15,7%), Тыве и Новосибирской области (15,3%), а также в Тверской области (14,5%). Следует отме-

тить, что эти статистические данные весьма приблизительные. К ним следует относиться с достаточной осторожностью, поскольку система статистического учета киберпреступлений пока далека от идеала в связи с тем, что процедура официального декларирования и подтверждения фактических финансовых потерь, причиненных в результате их совершения российским организациям, учреждениям, предприятиям и гражданам, все еще находится в стадии формирования.

В настоящее время в связи с развитием информационно-телекоммуникационных технологий, активно внедряющихся во все сферы человеческой деятельности, все чаще стали выделять специфические следы, возникающие в искусственно созданной на основе компьютерных систем среде электронно-цифрового отображения.

Существенной особенностью такой ситуации является то, что реальный объект или процесс окружающей действительности воспринимается субъектом уголовно-процессуального исследования не напрямую, а через посредство формализованной (математической) модели, с помощью которой этот реальный объект описывается. Поскольку формализованную модель человек строит, исходя из своих целей и задач, то она закономерно охватывает далеко не все элементы, свойства и поведение реального объекта, детально отражая лишь те из них, которые отвечают потребностям создателя искусственной среды отражения.

При этом в материальном виде (в виде числового набора) фиксируются лишь параметры используемой формализованной модели. Практически все ученые, исследующие механизм следообразования в виртуальном пространстве, признают его специфику и отличие возникающих при этом следов от всех иных видов рассматривавшийся ранее криминалистикой. Вместе с тем четко сформулировать, в чем это отличие выражается и как все это кратко назвать, остается вопросом, по которому существует множество различных точек зрения. В специальной литературе эти новые следы именуют бинарными, информационными, компьютерными, компьютерно-техническими, цифровыми и электронно-цифровыми (электронными) следами.

По нашему мнению, указанные следы рационально именовать виртуальными следами, поскольку это понятие наиболее полно отражает факт использования формализованной модели для искусственного построения всех интересующих создателя искусственной среды отражения проявлений наблюдаемого объекта или явления. Контур формирования виртуальных следов представляется наиболее сложным среди иных перечисленных выше, поскольку задействует искусственную среду отображения реальных объектов и явлений (построенную на основе компьютерных систем), а также среду взаимодействия компьютерных систем [3, с. 31].

Восприятие возникающей в контуре виртуальных следов информации осуществляется субъектом уголовно-процессуального исследования методами декодирования и интерпретации числовых наборов данных. Сложная картина совместного и взаимосвязанного формирования материальных, идеальных и виртуальных следов формирует целый спектр особенностей механизма следообразования, которые создают основу предмета изучения цифровой криминалистики.

Заключение

Таким образом, электронную цифровую информацию можно определить, как информацию, зафиксированную любым способом, но трансформируемую в человекочитаемый вид с помощью электромагнитных взаимодействий и кодированную с использованием цифрового кода, пригодную для автоматической обработки, находящуюся в информационно-технологических устройствах и передаваемую между ними любым способом либо распределенную между ними. Кроме определения круга информации, отграничения изучаемых действующих информационно-технологических объектов от разработок, находящихся в далекой перспективе и требующих иных методов исследования (а явно к квантовым, оптическим, биологическим и иным перспективным направлениям разработки альтернативных устройств не будут применимы имеющиеся рекомендации в связи со спецификой их работы, курсирования информации и круга решаемых задач), предлагаемый здесь подход позволит всесторонне учесть специфику объекта теоретических исследований и унифицировать следственно-судебную практику, устранив ошибки и разночтения, связанные с различными подходами к дифференциации электронных и цифровых устройств [5, с. 124].

Библиографический список

1. Смушкин А.Б. Объект и предмет электронной цифровой криминалистики // Технологии XXI века в юриспруденции: мат-лы 2-й междунар. науч.-практ. конф. (Екатеринбург, 22 мая 2020 г.) / под ред. Д.В. Бахтеева. Екатеринбург: Уральский государственный юридический университет, 2020. С. 530-541.

2. Обидин К.В. О роли электронной информации в уголовном судопроизводстве в условиях цифровизации // Вестник Университета имени О.Е. Кутафина. 2020. № 10 (74). С. 231-236.

3. Беломытцев Н.Н. Криптовалюта как предмет хищения путем использования компьютерной техники // Использование криптовалют в противоправных целях и методика противодействия: мат-лы междунар. науч.-практ. кругл. стола (Москва, 25 апр. 2019 г.) / под общ. ред. А.М. Багмета. М.: Московская академия Следственного комитета Российской Федерации, 2019. С. 16-22.

4. Пастухов П.С. Информационно-технологические устройства электронных доказательств / Основы теории электронных доказательств: монография / под ред. д-ра юрид. наук С.В. Зуева. М.: Юрлитинформ, 2019. С. 31-62.

5. Сукманов В.О. Сущность, понятие и виды электронно-цифровых следов, используемых в раскрытии и расследовании преступлений // Вестник Калининградского юридического института МВД России. 2020. № 4 (22). С. 124-127.