Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2023. – Т. 9 (75). № 2. – С. 294–298.

УДК 343.98

КРИМИНАЛИСТИЧЕСКОЕ РАСПОЗНАВАНИЕ В ТАКТИКЕ ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Даниленко Ю. А.
ФГАОУ ВО «КФУ им. В. И. Вернадского»

В статье проведено исследование криминалистического распознавания в тактике производства следственных действий при расследовании преступлений в сфере компьютерной информации. Большое внимание уделено компьютерной криминалистике, т.к. при расследовании киберпреступлений применяются такие следственные действия, которые являются индивидуальными, в частности осмотр места происшествия, проведение обыска и компьютерно-технической экспертизы.

Ключевые слова: преступление, криминалистика, электронно-цифровые следы, интернет, возбуждение уголовного дела, следствие, следственные действия.

Отдельные вопросы криминалистических тактик рассматриваются учеными с точки зрения разных подходов, поскольку единый подход не был выработан. Тактика производства следственных действий отражена в содержании криминалистической тактики. Эту процедуру рассматривают с точки зрения разных подходов.

Понятие тактики следственных действий, в контексте проведения расследования по преступлениям в сфере компьютерной информации в частности, толкуют с разных точек зрения.

Определенной системой обладает криминалистическая тактика, которая выступает разделом криминалистики. Содержание криминалистической тактики отражает С.А. Величкин. В частности, он раскрывает это понятие с точки зрения теоретических основ и практических мероприятий. «Теоретические основы включают понятийный аппарат, криминалистическую тактику, а также ее систему и задачи, объяснение понятия тактических приемов и тех требований, которые к ним предъявляются. Также обозначено, какую роль в этом процессе играют правовые, гуманитарные науки, следственная практика и по какому принципу происходит создание, формирование и разработка тактических приемов.

Практические рекомендации состоят в проведении отдельно выделенных следственных действий, а также в эффективном расследовании вышеуказанных категорий преступлений» [1]. Формирование двух автономных элементов в системе криминалистической тактики выделяют Е.П. Ищенко и Н.Н. Егоров. Речь идет о научных положениях и приемах, разработанных на их основе рекомендаций в отношении того, каким образом отдельные следственные действия могут быть организованы и надлежащим образом произведены [2].

Тактическая комбинация, тактическая рекомендация, тактический прием – это основные категории в криминалистической тактике. Получение компьютерной информации – это одно из основных следственных действий, которые производятся на этапе расследования киберпреступлений. На это обращают внимание большинство дознавателей, следователей и оперативных уполномоченных.

Однако, в отдельный раздел не выделена тактика производства следственных действий в компьютерной криминалистике. При расследовании киберпреступлений

рассматривают такие следственные действия, которые индивидуальны и присуще только этой отрасли. В частности, речь идет об осмотре места происшествия, проведении обыска и компьютерно-технической экспертизы.

Есть определенные особенности, которые указывают на главные отличия виртуальных следов от материальных следов, к чему удалось прийти на основании результатов анализа научной литературы.

В частности, речь идет об электронно-цифровом отражении, применении цифрового носителя для того, чтобы фиксировать информацию и нарушения.

Специалисты выделяют дорожку электронно-цифровых следов. Она формируется, если рассматривать информационно-телекоммуникационные сети в качестве орудия совершения преступлений в сфере компьютерной информации. Эта дорожка электронно-цифровых следов помогает распознать признаки преступлений, а также отразить главные обстоятельства произошедшего события.

Дорожка электронно-цифровых следов представлена в качестве системы образования следов в компьютерной сети. Она включает в себя записи о том, какая компьютерная информация прошла по линиям посредством коммутационного оборудования операторов связи, пересекая путь от компьютера преступника до компьютера потерпевшего. К указанной дорожке относятся записи, отражающие передвижение логически взаимосвязанной и последовательной информации. Таким образом, дорожки электронно-цифровых следов – это непосредственно система образования следов в пределах компьютерной сети.

Определённые методологические предпосылки служат основой на этапе формирования понятия следа в разрезе компьютерной криминалистики. На основании вышеуказанной информации, эти предпосылки представлены такими положениями: «след — это отражение деятельности киберпреступника; след — это интегративная система, отражающая особенности личности киберпреступника, процесса или действия компьютерной системы при совершении киберпреступлений; след как процесс и результат взаимодействия субъекта с объектом находит свое отражение как на материальных объектах, так и в сознании людей, а также и в киберпространстве» [3, с. 90].

На основании положений данного предлагаемого подхода напрашивается определенный вывод. В частности, след удается определить в качестве интегративной информационной системы. Интегративная информационная система сполна отражает деятельность личности преступника и тех лиц, которые тем или иным образом задействованы в преступлениях, совершенных в киберпространстве.

При совершении киберпреступления имеет место быть возникновение различных следов. Сформулированное выше понятие раскрывает все эти виды следов, выделяя основные элементы.

Единая классификация следственных действий в криминалистике отсутствует. К этому мнению удалось прийти, проанализировав большой объем специальной литературы. Авторы классифицируют следственные действия по разным основаниям, рассматривая суть и сущность этого понятия исходя из своих внутренних убеждений. Определено, что современный кратный рост количества компьютерных преступлений не может быть признан исключительно результатом случайного взаимодействия людей в силу повышения степени доступности информационных технологий (снижения стоимости персональных компьютеров, услуг доступа в сеть Интер-

нет и т.д.) либо результатом целенаправленной деятельности (движение «хакеров») по поиску способов несанкционированного доступа к компьютерам.

Разное количество квалификационных признаков приводится даже в том случае, когда следственные действия классифицируются по одному лишь основанию. На этапе расследования киберпреступлений, классификация следственных действий на вербальные и невербальные – это недостаточная классификация. Это связано с тем, что потребуется включение в классификацию отдельно выделенных следственных действий, которые необходимы для того, чтобы получить необходимую виртуальную информацию.

Д.С. Хижняк, одним из первых, рассматривает в диссертационном исследовании главные основания подходов к классификации следственных действий. Он обращает внимание на то, что, представляя классификации, учетные не обращают внимание на следственные действия, которые необходимы для того, чтобы виртуальная информация получила широкое распространение. Именно поэтому он вынес предложение о выделении тех следственных действий, которые необходимы для получения виртуальной информации [4].

Проблематичным является определение киберпреступления. По этой причине, можно наблюдать высокий уровень латентности преступлений в отрасли IT. Единой программы борьбы с киберпреступлениями в нашей стране нет.

Раскрытие, расследование киберпреступлений для сотрудников органов предварительного расследования вызывает массу сложностей, которые возникают на этапе сбора доказательств, доказывания информации, изучения виртуальных следов.

Исходя из изложенного, при расследовании киберпреступлений с учётом разработки тактических приёмов следственных действий необходимо проводить их классификацию по таким основаниям: «вербальные следственные действия; невербальные следственные действия; следственные действия, направленные на получение виртуальной информации (осмотр носителей электронной информации на наличие виртуальных следов; следственный эксперимент; обыск, выемка носителей электронной информации; назначение компьютерно-технической экспертизы» [5, с.78].

Самым рациональным способом действия следователя является ведение тактического приема. Также на этапе собирания, исследования, использования доказательной информации — это наиболее правильная линия поведения следователя. Развитие науки и передовой практики, а также полученные при этом данные и информация — это тактическая рекомендация. Тактическая рекомендация выступает организованным, целесообразным производством действий со стороны следователя. В данном случае, он занимается получением, исследованием и использованием доказательственной информации.

Тактический прием – это главная суть тактики производства следственного действия. К этому выводу можно прийти, принимая за основу вышеуказанные подходы.

Своими определенными особенностями обладают тактические приемы, используемые при проведении производства следственных действий в отношении расследования киберпреступлений. Владение следователем знаниями компьютерной криминалистики способствует эффективному применению определенных тактических приемов. Если лица, к компетенции которых относится выявление и раскрытие преступлений, недостаточно компетентны в данных вопросах, то это выступает существенной проблемой на этапе раскрытия киберпреступлений.

Зачастую возникает необходимость обратиться к криминалистическому распознаванию следовой картины. Это связано с тем, что определенной специфичностью обладает следовая картина киберпреступлений. Для ее формирования и решения необходимы принципиально новые методы, и средства.

Выявление новой, неизвестной информации в отношении расследуемого преступления – с этими сложностями сталкивается следователь на этапе расследования киберпреступлений. Также, порой сложно определить основные признаки соответствия или несоответствия поступающей информации и действительности.

«Применяя криминалистическое распознавание в ходе предварительной проверки сообщения о совершённом киберпреступлении, следователь: 1) «получает полное представление о характере деятельности и структуре объекта, где, возможно, было совершено преступление; 2) изучает конкретные условия деятельности объекта; 3) существующий порядок учёта и отчётности, систему документооборота; 4) выясняет коммуникативные и иные тактико-технические характеристики используемой компьютерной техники и программного обеспечения; 5) узнает организацию охраны объекта информатизации и конкретной компьютерной информации, а также служебные обязанности лиц, имеющих санкционированный доступ к охраняемой законом компьютерной информации, прямое или косвенное отношение к ценностям, которые стали предметом преступного посягательства» [6, с. 89].

«Криминалистическое распознавание применяется также при выявлении следов, остающихся после совершения киберпреступлений. Следы при совершении киберпреступлений, зачастую, различаются, однако, их можно разделить согласно приведённой классификации следственных действий» [4, с. 89].

Расширение круга объектов-носителей информации – необходимая мера на этапе выявления следов. Данная информация должна отражать произошедшие преступные события, его отдельные элементы, а также квалификацию лиц, задействованных в данном преступлении. Сам факт совершения преступление, его отдельные элементы отражаются в сознании субъектов преступления, в сознании иных лиц, но одновременно с этим, подчиняются определенным закономерностям.

На этапе производства следственных действий по киберпреступлениям, на основании всей вышеизложенной информации, стоит обратить внимание на три основных вида криминалистического распознания.

В частности, речь идет о непосредственном распознавании, опосредованном распознавании, распознавании виртуальной информации с применением специальных технических средств. Непосредственное распознавание – это определение признаков неправдивой информации на этапе получения показаний. Опосредованное распознавание – это анализ выводов, к которым пришли эксперты и специалисты на этапе предварительного следствия. Таким образом, понятие угрозы безопасности информационных сетей имеет четкое определение. В частности, речь идет о негативных последствиях потенциально или реально совершенных действий, событий. В частности, данные, находящиеся в информационной системе, могут неправомерно, нелегально использоваться и уничтожаться.

Получение компьютерной информации – это одно из основных следственных действий, которые производятся на этапе расследования киберпреступлений.

Криминалистическая теория и практика нуждается в постоянном совершенствовании механизмов, обладающих способностью к обнаружению и расследованию

преступлений, совершенных в сфере компьютерной информации. На это, в частности, направлены все последующие разработки и внедрение теоретических основ классификации киберпреступлений, повышение профессиональных навыков процессуальных субъектов, уполномоченных проводить предварительное расследование по данному виду преступлений и т.д.

Список литературы:

1. Величкин, С. А. Криминалистическая тактика / С. А. Величкин, Я. С. Величкин. – Москва : Издательство "Юрлитинформ", 2019. – 264 с. – (Библиотека криминалиста). – ISBN 978-5-4396-1836-1. – EDN ZDMLQT.
2. Ищенко Е.П. Современные технико-криминалистические средства, применяемые для обнаружения доказательств на электронных носителях информации (в соавторстве с Костюченко О.Г.) в журнале Вестник Восточно-Сибирского института МВД России, издательство Федеральное государственное казенное образовательное учреждение высшего образования Восточно-Сибирский институт Министерства внутренних дел Российской Федерации (Иркутск), № 2 (97), с. 181-189 (2021)
3. Косарев М.Н. Информационно-телекоммуникационные сети как признак преступления /М.Н. Косырев // Вестник Уральского юридического института МВД России. 2014. № 4. С. 55–56 – Текст: непосредственный
4. Хижняк Д.С. Методологические основы расследования транснациональных преступлений: модельный подход : автореф. дис. ... д. юрид. наук. – Москва, 2018. – 45 с. – Текст: непосредственный
5. Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет : автореф. дис. ... канд. юрид. наук. – Саратов, 2018. – 25 с. – Текст: непосредственный
6. Гаврили Ю.В. Практика организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий /Ю.В.Гравили / Труды Академии управления МВД России. 2018. № 4 (48). С. 148–149– Текст: непосредственный.

Danilenko Yu. A. Criminalistic recognition in the tactics of producing investigative actions in the investigation of crimes in the sphere of computer information // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2023. – T. 9 (75). № 2. – P. 294–298.

The article studies forensic recognition in the tactics of investigative actions in the investigation of crimes in the field of computer information. Much attention is paid to computer forensics, because when investigating cybercrime, such investigative actions are used that are individual, in particular, inspection of the scene, conducting a search and computer-technical expertise

Keywords: crime, criminology, digital traces, Internet, initiation of a criminal case, investigation, investigative actions.

Spisok literatury:

1. Velichkin, S. A. Kriminalisticheskaya taktika / S. A. Velichkin, YA. S. Velichkin. – Moskva : Izdatel'stvo "YUrlitinform", 2019. – 264 s. – (Biblioteka kriminalista). – ISBN 978-5-4396-1836-1. – EDN ZDMLQT.
2. Ishchenko E.P. Sovremennye tekhniko-kriminalisticheskie sredstva, primenyaemye dlya obnaruzheniya dokazatel'stv na elektronnyh nositelyah informacii (v soavtorstve s Kostyuchenko O.G.) v zhurnale Vestnik Vostochno-Sibirskogo instituta MVD Rossii, izdatel'stvo Federal'noe gosudarstvennoe kazennoe obrazovatel'noe uchrezhdenie vysshego obrazovaniya Vostochno-Sibirskij institut Ministerstva vnutrennih del Rossijskoj Federacii (Irkutsk), № 2 (97), s. 181-189 (2021)
3. Kosarev M.N. Informacionno-telekommunikacionnye seti kak priznak prestupleniya /M.N. Kosyrev // Vestnik Ural'skogo yuridicheskogo instituta MVD Rossii. 2014. № 4. S. 55–56 – Tekst: neposredstvennyj
4. Hizhnyak D.S. Metodologicheskie osnovy rassledovaniya transnacional'nyh prestupleniĭ: model'nyĭ podhod : avtoref. dis. ... d. yurid. nauk. – Moskva, 2018. – 45 s. – Tekst: neposredstvennyj
5. Komarov A.A. Kriminologicheskie aspekty moshennichestva v global'noj seti Internet : avtoref. dis. ... kand. yurid. nauk. – Saratov, 2018. – 25 s. – Tekst: neposredstvennyj
6. Gavrili YU.V. Praktika organizacii vzaimodejstviya pri rassledovanii prestuplenij, sovershennyh s ispol'zovaniem informacionno-kommunikacionnyh tekhnologij /YU.V.Gravili / Trudy Akademii upravleniya MVD Rossii. 2018. № 4 (48). S. 148–149– Tekst: neposredstvennyj.

.