Научная статья
УДК 343.98:004
doi 10.46741/2713-2811.2024.25.1.013

Концептуальные положения криминалистической методики расследования преступлений в сфере киберпространства

ОЛЕГ СТАСЬЕВИЧ КУЧИН

Российский государственный университет правосудия, Москва, Россия, kuchin-os@rambler.ru, https://orcid.org/0000-0001-7604-6011

Аннотация. Разработка концептуальных положений расследования преступлений в сфере киберпространства позволяет формализовать их существенную часть, что обеспечивает возможность создания групповой методики расследования этих преступлений. При этом речь идет также о разработке единой криминалистической характеристики преступлений данной группы и формировании совокупности таких характеристик, имеющих однотипную структуру.

Ключевые слова: преступление; киберпространство; криминалистика; расследование; криминалистическая методика; нейросети; уголовное право; IT-технологии.

5.1.4. Уголовно-правовые науки.

Для цитирования: Кучин О. А. Концептуальные положения криминалистической методики расследования преступлений в сфере киберпространства // Ius publicum et privatum: сетевой научно-практический журнал частного и публичного права. 2024. № 1 (25). С. 103–112. doi 10.46741/2713-2811.2024.25.1.013.

Original article

Conceptual Provisions of the Forensic Methodology for Investigating Cyber Crimes

OLEG S. KUCHIN

Russian State University of Justice, Moscow, Russia, kuchin-os@rambler.ru, https://orcid.org/0000-0001-7604-6011

Abstract. The development of conceptual provisions for the investigation of crimes in the field of cyberspace makes it possible to formalize their essential part, which makes it possible to create a group methodology for investigating these crimes. At the same time, we are also talking about the development of a unified forensic characteristic of crimes of this group and the formation of a set of such characteristics with a similar structure.

Keywords: crime; cyberspace; criminalistics; investigation; forensic methodology; neural networks; criminal law; IT technologies.

© *Кучин О. А., 2024*

5.1.4. Criminal law sciences.

For citation: Kuchin O.A. Conceptual provisions of the forensic methodology for investigating cyber crimes. *Ius publicum et privatum: online scientific and practical journal of private and public law*, 2024, no. 1 (25), pp. 103–112. doi 10.46741/2713-2811.2024.25.1.013.

Разработка любых групповых (видовых, родовых и иных обобществленных) криминалистических методик расследования преступлений опирается на особенности процесса расследования как самих групп, так и отдельных преступлений. Это концептуальное положение однозначно применимо и к преступлениям, совершаемым в сфере киберпространства. В процессе следственной и судебной практики постоянно возникает ряд новых проблем, связанных со значительным разнообразием таких преступлений.

Основой разработки криминалистических методик расследования преступлений в сфере киберпространства являются их легальные признаки, изложенные законодателем в диспозициях статей Особенной части уголовного кодекса, определяющих соответствующую ответственность за эти деяния.

Анализ уголовно-правовых характеристик преступлений в сфере киберпространства показал, что применяемая в научной криминалистической литературе дефиниция «преступление в сфере киберпространства» с точки зрения положений уголовного права носит весьма условный и специфический характер. Такая же ситуация складывается и с иными криминалистическими видами или группами преступлений в любой сфере их совершения.

Основополагающей и составной частью всех объединенных криминалистических методик расследования преступлений является их криминалистическая характеристика, основанная на развернутой уголовно-правовой, криминологической, социологической, политической и оперативно-розыскной характеристике преступлений определенного вида или группы и соответствующих характеристиках обстоятельств, подлежащих установлению при расследовании уже конкретного преступления.

Следовательно, научная концепция криминалистических методик расследования преступлений в сфере киберпространства носит интегрированный характер и аккумулирует положения не только уголовно-правовых, но и ряда наук информационно-кибернетического блока.

Быстрый рост преступлений в сфере киберпространства в настоящее время связан с активным использованием компьютерной техники, разнообразных компьютеризованных устройств и информационных технологий.

Переход преступников к использованию информационного пространства нейросетей, в котором действует довольно сложная система передачи информации, сопровождается рядом принципиально новых явлений, связанных с ментальными изменениями сознания и личного психического отношения к ним со стороны пользователей сети Интернет, а также почитателей различных IT-технологий. Они проявляются при криминалистическом исследовании различных возрастных и социальных групп людей, постоянно использующих компьютерную технику и информационные технологии. Полученные специалистами результаты и выводы научных исследований позволяют установить ряд специфических особенностей менталитета и поведения активных пользователей сети Интернет.

Российский законодатель криминализовал пока только лишь несколько деяний в сфере компьютерной информации, включив в гл. 28 УК РФ всего четыре состава. Но следует

отметить, что уже во многие составы преступлений внесены квалифицирующие признаки, которые прямо указывают на использование виновными лицами компьютерной техники, информационных технологий и Интернета.

Российские специалисты в области криминалистики давно отмечают, что признаки использования IT-технологий рассредоточены в настоящее время по многим составам преступлений, изложенным в УК РФ. Поэтому для преступлений в сфере киберпространства характерны проявления множественности их совершения. И хотя данная группа общественно опасных деяний пока еще не выделена в отдельную главу УК РФ, но, как уже указывалось нами ранее, соответствующие криминальные проявления отмечаются в нескольких десятках различных составов преступлений.

Преступные деяния в сфере киберпространства надлежит выделить в отдельную криминалистическую группу. И, следовательно, для преступлений данной криминалистической группы необходимо разработать групповую криминалистическую характеристику как основную, концептуальную составную часть криминалистической методики ее расследования.

Специалистами отмечается, что многие примеры криминального поведения в сфере киберпространства представляют собой одинаковые повторяющиеся преступления, совершенные разными лицами.

Так, например, к таким преступлениям относятся публичные призывы к осуществлению экстремистской деятельности, совершенные с использованием электронной почты или СМС-сообщений по мобильной телефонной связи от одного лица к другому или нескольким лицам. При этом во многих случаях речь идет не только об экстремизме, но и о призывах к массовым беспорядкам и иным тяжким преступлениям. Ряд экстремистских преступлений в сфере киберпространства характеризуются сложным составом и определенной формой соучастия двух и более лиц.

Согласимся с мнением некоторых специалистов, что исследование в данной области должно быть направлено не только на формирование единой криминалистической характеристики группы преступлений в сфере киберпространства и их совокупностей, но и на формирование совокупности таких характеристик, имеющих однотипную структуру.

Структура информационного наполнения криминалистических характеристик преступлений данной категории должна быть разработана на основе развернутых уголовно-правовых характеристик и обстоятельств, подлежащих установлению, а также накопленного судебно-следственного опыта и различных эмпирических данных. Именно такой научный подход необходим для формирования криминалистических характеристик различных видов преступлений в сфере киберпространства как основы частных криминалистических методик их расследования.

В науке обоснованно отмечается тот факт, что необходимо создавать объемные описания криминалистических характеристик преступлений данной группы и уже на их основе создавать подробные частные методики их расследования.

Выявление, раскрытие и расследование преступлений в сфере киберпространства, должны совершаться не только с применением традиционных криминалистических технологий, но и новых возможностей, алгоритмов и программ, позволяющих создать соответствующие компьютерные модели криминалистических характеристик этих преступлений и их совокупностей.

Криминалистические методики расследования преступлений в сфере киберпространства концептуально нацелены на раскрытие содержательных особенностей отдельных на-

правлений расследования, выдвижение и обоснование следственных версий с их последующей проверкой, а также выполнение конкретных следственных действий.

Необходима постоянная разработка криминалистических тактических приемов соответствующих следственных действий с электронными носителями цифровой информации, электронными документами и иной электронной продукцией текстового и графического характера. При этом определенное внимание должно уделяться применению разумных тактических рекомендаций для работы с закодированной и зашифрованной электронной информацией, имеющей правовой статус, в рамках криминалистических методик расследований и современных информационных технологий, включая элементы искусственного интеллекта.

Многие специалисты предлагают осуществлять разработку научно обоснованных подходов для формирования комплекса криминалистических методик для всех преступлений в сфере киберпространства.

На основе нескольких таких методик и с учетом особенностей соответствующей криминалистической характеристики конкретного преступления данного вида следователь сможет сформировать частную криминалистическую методику, адаптированную для расследования конкретного криминального факта в сфере киберпространства или их определенной совокупности.

Для формирования научных основ частных криминалистических методик, выверенных с правовой точки зрения, были проведены исследования различных подходов к обоснованию требований по структуре и содержанию частных криминалистических методик. Ряд специалистов предлагает сократить структуру частных криминалистических методик расследования преступлений до четырех элементов: криминалистическая характеристика данного вида преступления; типичные следственные ситуации и программы расследования; тактика отдельных следственных действий и оперативно-розыскных мероприятий; организация профилактической деятельности следователя при расследовании данных преступлений [1].

Мы категорически не согласны с такой позицией.

Вместе с тем В. О. Давыдов обоснованно предлагает определить базовую методику расследования как совокупность разработанных криминалистической наукой и апробированных в следственной практике комплексов методических рекомендаций по расследованию преступлений, сформированных на основании их уголовно-правовой и криминалистической классификаций и предназначенных для оптимизации и повышения эффективности работы следователя [2].

Подобная методика расследования является базовой и комплексной, представляя собой совокупность выработанных криминалистической наукой и апробированных следственной практикой методических рекомендаций по выявлению, раскрытию и расследованию криминалистическими средствами и методами преступлений, объединенных в единый предмет исследования [2].

Структура данной методики включает в себя следующие элементы: криминалистическая характеристика преступной деятельности в сфере киберпространства; комплекс рекомендаций по разрешению типичных следственных ситуаций и сопутствующих им задач начального и последующего этапов расследования; комплекс рекомендаций по решению информационных задач и версионной работе по делам данной группы; комплекс рекомендаций по планированию и организации расследования; комплекс рекомендаций по взаимодействию следователя с оперативно-розыскными подразделениями как при их

раздельной деятельности, так и в рамках совместных следственно-оперативных групп, а также с правоохранительными органами иностранных государств и международными полицейскими организациями; комплекс рекомендаций по назначению судебных экспертиз; комплекс рекомендаций по проведению отдельных следственных действий и тактических операций на первоначальном и последующих этапах расследования; комплекс рекомендаций по взаимодействию субъекта расследования со средствами массовой информации, в том числе и сети Интернет, а также по использованию помощи общественности; комплекс рекомендаций по предупреждению преступлений в сфере киберпространства на территории Российской Федерации средствами и методами криминалистики [2].

При этом криминалистическая характеристика преступной деятельности в сфере киберпространства представляет собой систематизированное описание массива фактических данных и основанных научных выводов о наиболее типичных криминалистически значимых элементах, проявляющихся в механизме преступной деятельности в сфере киберпространства в территориальном диапазоне, знание которых необходимо для разработки соответствующей базовой частной методики расследования, определения перечня обстоятельств, подлежащих установлению, выдвижения следственных версий и определения основных направлений расследования.

Результат научного исследования, сделанного В. О. Давыдовым, позволяет говорить о том, что структура преступности в сфере киберпространства в целом должна соответствовать структуре механизма этой преступной деятельности и включать в себя типовые сведения о следующих элементах и взаимозависимостях между ними: субъект преступной деятельности (его организованные формы, а также ролевые функции и типологические свойства личности их руководителей, активных членов и иных лиц, оказавшихся косвенно связанных с субъектом преступной деятельности подобного вида); мотивы и цели; способы совершения преступной деятельности, в том числе включающие совокупность преступных действий по сокрытию следов, а также намеренному афишированию преступного результата; место создания региональных звеньев преступного формирования, действующих на территории Российской Федерации, и непосредственного осуществления ими преступной деятельности; обстановка, связанная с преступной деятельностью; типологические свойства личности и ролевые функции потерпевших; предметы преступного посягательства, с которыми связаны фактическое наступление вредных последствий и характер преступного результата; средства и орудия, используемые для совершения преступной деятельности рассматриваемой криминалистической группы, а также преступный результат [2].

Механизм преступной деятельности в сфере киберпространства представляет собой сложную динамическую систему, в которой следует выделить две группы способов:

1) базовые способы совершения основной преступной деятельности;

2) вспомогательные способы преступной деятельности.

Все они одинаково направлены на обеспечение функционирования элементов организационно-структурных криминальных модулей, включая и региональные звенья.

В качестве криминалистически значимых особенностей данных способов совершения преступных деяний следует выделить использование информационно-коммуникационных технологий и ресурсов сети Интернет, которые в силу своей прикладной специфики отличаются повторяемостью поведенческих актов и использованием информационно-коммуникационных технологий в целях организации и руководства деятельностью звеньев преступных формирований, создания условий для совершения ими преступных деяний в том или ином субъекте Российской Федерации.

В основе противодействия расследованию, реализуемого членами преступных группировок, лежат криминализированные связи как членов самого местного звена, так и функциональных звеньев иерархического организационно-структурного модуля, а его механизм складывается из совокупности действий, сочетание и последовательность которых варьируются в зависимости от инициативы субъекта противодействия, этапов расследования, особенностей способов противодействия, их комбинаций и др. и охватывает противодействие расследованию, осуществляемое непосредственно сразу после совершения преступления в сфере киберпространства, осуществляемое после возбуждения уголовного дела и на последующих стадиях его расследования.

Неотъемлемым элементом механизма преступной деятельности в сфере киберпространства является комплекс действий, направленных в подавляющем большинстве случаев на совершение преступления высокотехнологичными способами, связанными с использованием информационно-коммуникационных сервисов сети «Интернет».

Преступная мотивация представляет собой субъективную детерминирующую систему взаимосвязанных элементов, характеризующих субъект преступной деятельности и другие ее составляющие, на основе изучения закономерностей возникновения и развития криминальных процессов.

Цель преступной деятельности в сфере киберпространства выступает как мысленная модель идеально представляемого и желаемого преступного результата, к достижению которого стремится лицо, совершающее преступление рассматриваемой группы.

Однозначно необходимо обратить внимание на специфические особенности преступности в сфере киберпространства, установленные по результатам исследований и накопленного эмпирического материала. Полученные результаты предопределили ряд акцентов в дальнейших разработках особенностей совершения данных преступлений в разных социальных группах, а также различных проявлений множественности преступлений данного вида. Безусловно, в рамках выявленных особенностей проявляется и ряд внешних факторов, оказывающих существенное влияние на количественное и качественное изменение динамики преступных проявлений данной группы.

Считаем, что при разработке научно-методических основ для создания и формирования частных криминалистических методик расследования преступлений в сфере киберпространства и их совокупностей возможно использовать ряд элементов методических разработок, предложенных В. О. Давыдовым [2].

Одновременно В. В. Бычков и В. А. Прорвич выделяют следующие структурные элементы комплекса тех информационных технологий, которые могут быть заложены в основу базовой иерархической системы, позволяющей осуществлять формирование адаптировных частных криминалистических методик расследования преступлений в сфере киберпространства или их совокупностей:

1. Информационные технологии, позволяющие контролировать процессы формирования электронных документов и иных сведений, в различных информационных системах, отражающих особенности субъектно-объектных и субъектно-субъектных отношений в информационном пространстве компьютерных сетей, включая Интернет, на предмет установления их соответствия либо несоответствия требованиям действующего законодательства и формирования информационных эталонов соответствующей деятельности законопослушных субъектов.

2. Информационные технологии, нацеленные на надлежащее раскрытие бланкетных, отсылочных и смешанных диспозиций уголовно-правовых норм по преступлениям в сфере киберэкстремизма и их совокупностей с различными формами соучастия, для формирования развернутых уголовно-правовых характеристик преступлений, совершаемых в информационном пространстве компьютерных сетей, позволяющих выделить полную совокупность обязательных и факультативных признаков конкретных преступлений рассматриваемого вида и их совокупностей, а также перечень обстоятельств, подлежащих доказыванию, ориентирующих следствие на поиск криминалистически значимой информации на различных стадиях доследственной проверки и производства по соответствующим уголовным делам о преступлениях в сфере киберэкстремизма.

3. Информационные технологии, нацеленные на сопоставление электронных документов и сведений из различных информационных систем со сформированными информационными эталонами в последовательно-параллельном режиме, для выявления закодированных информационных следов противоправных действий определенных субъектов, имеющих признаки преступлений определенного вида, и их фиксации, для последующего построения и обоснования следственных версий и формирования доказательств по расследуемому уголовному делу.

4. Информационные технологии, нацеленные на сопоставление определенных групп электронных документов и сведений из различных информационных систем со сформированными информационными эталонами в последовательно-параллельном режиме для выявления распределенных закодированных информационных следов противоправных действий определенных субъектов, имеющих признаки преступлений в сфере киберпространства, их совокупностей, и их фиксации для последующего построения и обоснования следственных версий и формирования доказательственной базы.

5. Информационные технологии, нацеленные на создание интерактивных экспертных систем с элементами искусственного интеллекта различного вида, позволяющих следователю при обработке информации, имеющей правовой статус, в диалоговом режиме контролировать сохранение статуса промежуточных и итоговых результатов ее обработки.

6. Информационные технологии, нацеленные на надлежащее применение специальных знаний и профессиональных компетенций судебных экспертов и специалистов, включая созданные на их основе алгоритмы обработки информации, имеющие правовой статус, реализованные сведущими лицами в форме проблемно ориентированных компьютерных программ, предназначенных для использования в диалоговых режимах различного формата в составе интерактивных экспертных систем.

7. Информационные технологии, нацеленные на создание интерактивных экспертных систем с элементами искусственного интеллекта различного вида, позволяющих следователю при расследовании преступлений в сфере киберпространства и их совокупностей организовать коллективную обработку информации, имеющей правовой статус, в параллельно-последовательном режиме со специалистами и судебными экспертами, с применением средств контроля за сохранением правового статуса промежуточных и итоговых результатов ее обработки [3].

Соответствующие методы обработки документированной электронной информации должны обеспечивать контроль за сохранением промежуточных и итоговых результатов.

Основным назначением таких методов является выделение той части сведений, имеющихся в электронной документации, которые имеют признаки криминала, на фоне намного большей по объему информации, отражающей правомерные действия граждан.

Если же речь идет о целенаправленной обработке электронной документации, изъятой следователем из определенных информационных систем, чтобы выявить в ней ту часть, которая имеет признаки криминального характера, то вполне понятно, что и соответствующие следы также носят закодированный информационный характер. Такие следы могут носить не информационно-замкнутый характер, поддающийся интерпретации для установления определенных фактов и обстоятельств, а фрагментарный, не отражающий характеристику определенного события, которое может идентифицироваться как криминальное. При этом соответствующие фрагменты могут быть рассеяны по различным электронным документам, а для их идентификации и установления информационного следа криминального события необходима целенаправленная, проблемно-ориентированная обработка определенных групп документов, в том числе с использованием информационных эталонов законопослушной деятельности.

Электронные документы создаются, хранятся, передаются и преобразовываются в том числе и в другие электронные документы с помощью определенных компьютерных программ, которые принято называть также компьютерными кодами. Соответственно, определенные фрагменты криминальной информации, которые могут быть выявлены и зафиксированы в некоторой совокупности электронных документов, могут идентифицироваться как закодированные информационные следы преступлений рассматриваемого вида.

С помощью соответствующих методов на основе выявленных в определенной совокупности электронных документов и зафиксированных закодированных информационных следов преступлений могут быть идентифицированы их связи с соответствующими информационными системами и их обладателями. Это позволяет сформировать на их основе доказательства, изобличающие определенных лиц в причастности к расследуемым высокотехнологичным преступлениям.

Методы обработки электронных документов могут сочетаться с иными способами обработки документации на бумажных носителях информации, а также, например, с алгоритмами выполнения отдельных видов следственных действий. Это позволяет использовать прямые и обратные связи таких действий для получения кумулятивного эффекта, что повышает эффективность расследования соответствующих уголовных дел.

Отталкиваясь от сформированных таким образом обязательных и факультативных признаков преступлений в сфере киберпространства, с помощью уже обсуждавшихся подходов, основанных на специальных знаниях и элементах искусственного интеллекта, разработанных в рамках информатики, можно построить методы обработки текстовых формулировок тех положений законодательства, которые необходимы для раскрытия содержательных особенностей диспозиций конкретных уголовно-правовых норм.

В ряде случаев с помощью указанных алгоритмов и на основе выявленных признаков можно идентифицировать наличие не одного, а двух и более совершенных преступлений в сфере киберпространства, что предполагает в дальнейшем планирование и производство дополнительных следственных действий.

Важно обратить внимание и на то, что подобные информационные технологии, позволяющие целенаправленно анализировать текстовую информацию с использованием определенной системы критериев и информационных эталонов, уже существуют и актив-

но используются в ряде отраслей человеческой деятельности. На их основе может быть разработана система алгоритмов различного вида, матричных классификаторов и иного компьютерного инструментария, позволяющего обеспечить надлежащее информационное обеспечение всего комплекса следственных и иных процессуально регламентированных действий по преступлениям рассматриваемого вида.

Фактически речь идет о разработке и создании силами ученых и специалистов в различных отраслях права, экономики и информатики иерархической системы методов, позволяющих формализовать информационно-правовое пространство, характеризующее различные варианты деятельности законопослушных субъектов информационного общества различного вида и уровня. Научно обоснованное структурирование такого пространства позволит также создать определенную систему типовых действий законопослушных субъектов и использовать их в качестве эталонов при выявлении противоправных действий в различных сферах информационного общества.

Поэтому в настоящее время все более ощущается необходимость в научном обеспечении способов преобразования растущего количества криминалистически значимой информации в новое качество информационной модели исследуемых преступлений в сфере киберпространства. Здесь возникает ряд новых положений, согласно которым по признакам состава преступления компьютерные технологии обработки электронных документов позволяют получить значительно большее количество сведений, нежели с помощью других методов.

Все вышеизложенные положения должны составить современную концепцию криминалистической методики выявления, раскрытия и расследования преступлений в сфере киберпространства.

СПИСОК ИСТОЧНИКОВ

1. Возгрин И. А. Ведение в криминалистику. История, основы теории, библиография. СПб., 2003. С. 485.
2. Давыдов В. О. Методика расследования транснациональной преступной деятельности экстремистского характера : дис. … д-ра юрид. наук. Тула, 2018. С. 525–528.
3. Бычков В. В., Прорвич В. А. Алгоритмы выявления признаков экстремистской и террористической деятельности с использованием Интернета на основе информационных шаблонов возможных составов преступлений данного вида // Расследование преступлений: проблемы и пути их решения. 2022. № 2. С. 43–50.

REFERENCES

1. Vozgrin I.A. *Vedenie v kriminalistiku. Istoriya, osnovy teorii, bibliografiya* [Introduction to criminology. History, fundamentals of theory, bibliography]. Saint Petersburg, 2003. P. 485.
2. Davydov V.O. *Metodika rassledovaniya transnatsional'noi prestupnoi deyatel'nosti ehkstremistskogo kharaktera: dis. … d-ra yurid. nauk* [Methods of investigation of transnational extremist criminal activities: Doctor of Sciences (Law) dissertation]. Tula, 2018. Pp. 525–528.
3. Bychkov V.V., Prorvich V.A. Algorithms for detecting signs of extremist and terrorist activities using the Internet based on information templates of possible crimes of this type. *Rassledovanie prestuplenii: problemy i puti ikh resheniya = Investigation of Crimes: Problems and Solutions*, 2022, no. 2, pp. 43–50. (In Russ.).

СВЕДЕНИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

ОЛЕГ СТАСЬЕВИЧ КУЧИН – доктор юридических наук, профессор, академик Российской академии естествознания, профессор кафедры судебных экспертиз и криминалистики Российского государственного университета правосудия, Москва, Россия, kuchin-os@rambler.ru, https://orcid.org/0000-0001-7604-6011

OLEG S. KUCHIN – Doctor of Sciences (Law), Professor, Academician of the Russian Academy of Natural Sciences, professor at the Department of Forensic Enquiry and Criminalistics of the Russian State University of Justice, Moscow, Russia, kuchin-os@rambler.ru, https://orcid.org/0000-0001-7604-6011

Статья поступила 19.02.2024