УДК 343.3/.7

П. А. Гревцов, В. А. Митьков, А. А. Москаленко
Кузбасский государственный технический университет
им. Т.Ф. Горбачева, Кемерово, Россия

КРИМИНАЛИСТИЧЕСКИЕ ПОДХОДЫ К РАССЛЕДОВАНИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ IT-ТЕХНОЛОГИЙ

научный руководитель: д.ф.н., профессор кафедры истории, философии
и социальных наук Золотухин В.М.

Рост кибермошенничества, подделка электронно-цифровых подписей, взлом личных кабинетов граждан и юридических лиц, хищении паролей и т. д. актуализирует поиск методов, способов и механизмов борьбы с ними. В связи с этим возрастает роль применения криминалистических подходов расследованию преступлений в сфере IT-технологий. Подчеркивается, что криминалистические подходы, направленные на установление мотива совершения преступления в IT-сфере, связаны с установлением лиц возможно причастных к преступлению как работников предприятия, банка, в которых осуществлено преступления с применением IT-технологий либо сотрудников, которые обладали доступом к закрытым данным и впоследствии уволились.

Ключевые слова: кибермошенничество, IT-технологии, конфиденциальная информация, правонарушения, персональные данные.

Цифровизация практически всех секторов реальной экономики, внедрение современных IT-технологий существенно облегчает технологические процессы обмена информацией, банковских переводов [Бахов, Беккер, 2020; Золотухин, Козырева, 2021; Третьякова, 2021; Слонов, Козырева, 2022], а также участия в электронных формах торгов, заключении договоров с использованием электронно-цифровых подписей.

Вместе с тем существует и обратная сторона медали, выражающаяся в увеличении количества преступлений в IT-сфере, кибермошенничестве, подделки электронно-цифровых подписей [Количенко, 2022], взлома личных кабинетов граждан и юридических лиц, хищении паролей, CVV-кодов владельцев банковских карт и многих других форм компьютерных преступлений. В связи с этим, возникает проблема информационной безопасности [Гаврилов, 2020; Золотухин, Золотухин, 2022] и трансформации сознания [Труфанова, Хан, 2022; Gritskevich, Zolotukhin, Kazakov, 2019; Zolotukhin., Zhukova, 2019].

Компьютерным преступлением, или как сейчас принято называть преступление в сфере IT технологии, является преступление, совершенное с примене-

нием технологией информационно-телекоммуникационной сети Интернет и направленное на хищение чужого имущества, конфиденциальной информации, нарушение авторских прав, создание и распространение хакерских вредоносных программ, действия пранкеров по распространению в сети фейковой, недостоверной и порочащей интересы государства, общества и конкретных лиц информации.

Сегодняшние преступления в сфере IT-технологий разнообразны по своему содержанию, субъективной и объективной стороне уголовного правонарушения.

При этом такие преступления требуют особых криминалистических подходов при проведении расследования и установления преступных лиц, причастных к совершению таких противоправных действий с использованием IT-технологий [Багмет, Антонов, Бычков, 2020, с. 89].

Рассматривая и систематизируя применяемые на практике криминалистические подходы к расследованию правонарушений, которые были совершены с применением IT-технологий, обращает на себя внимание, что на каждом из этапов производства необходимы определенные следственные действия:

1. Осмотр места происшествия. Многие преступления в IT-сфере совершаются путем удаленного доступа с IP-адресов, которые зачастую находятся в иных городах чем место совершения преступления, а зачастую даже за пределами Российской Федерации. В последнее время участились подобные преступления с территории Украины.

В том же случае, когда удалось по IP-адресу найти место совершения преступления, необходимо привлечение в обязательном порядке для расследования специалиста, обладающего познаниями в сфере совершаемых киберпреступлений, поскольку следователь как процессуальная фигура будет просто бессилен в этой ситуации установить способ, средство, метод совершения преступления, поскольку не обладает знаниями в IT-сфере [Тюнис, 2020, С. 137; Ленев, 2022].

Помимо осмотра места преступления целесообразно изъятие компьютерной техники, при помощи которой вероятнее всего было совершено преступление.

2. Использование оперативно-розыскного взаимодействия с операторами сотовой связи, провайдерами оказания коммуникационных услуг с целью установления как средства совершения преступлений, IP адресов местонахождения компьютерной техники, с помощью которых осуществлено преступление, а также владельцев телефонных сим-карт сотовых операторов, при помощи которых было совершено преступное деяние. Распространенным примером подобных нарушений является лжебанковский сотрудник, который посредством мобильной связи узнает персональные данные по банковской карте у потерпевшего и осуществляет кражу денежных средств со счета.

Как показывает практика, зарегистрированы такие телефоны, по которым звонит преступник, в других регионах и на подставных лиц, но тем не менее задачей следователя является установление факта принадлежности мобильного номера телефона конкретному физическому лицу.

Провайдер или сотовый оператор может предоставить органам дознания и расследования интересующую их информацию [Маинов, 2022].

3. Оценка мотива совершения преступлений в сфере IT-технологий. Наиболее часто мотивом преступления в IT-сфере выступает корысть, желание заработать легким путем денежные средства как способом кражи их с банковского счета, карты, так и получения путем шантажа в результате имеющегося доступа к личным персональным данным, которые преступник грозится раскрыть в открытом доступе, если не будут выполнены его условия и требования.

Также мотивами преступления в IT-сфере могут быть зависть, ненависть, национальная вражда, пренебрежение к обществу и иные факторы, провоцирующие преступника на совершение противоправного деяния [Бертовский, 2021, С. 77; Золотухин, 2020, Золотухин, 2021].

Криминалистические подходы, направленные на установление мотива совершения преступления в IT-сфере, связаны с установлением лиц возможно причастных к преступлению как работников предприятия, банка, в которых осуществлено преступления с применением IT-технологий либо сотрудников, которые обладали доступом к закрытым данным и впоследствии уволились.

В этом случае криминалист осуществляет опрос свидетелей, осуществляет получение информации о порядке формирования и выдачи паролей к базам данных хозяйствующего субъекта, устанавливает порядок входа в систему данных, из которой осуществлена кража, утечка информации или похищены денежные средства.

4. Назначение экспертизы. Следователь в силу своего процессуального положения и объема профессиональных знаний в сфере юриспруденции не обладает познаниями в IT-технологиях, достаточными для установления способа и средства совершения преступления. Для этих целей в рамках расследования преступлений в сфере IT-технологий, которые отражены в главе 28 Уголовного кодекса РФ, привлекаются эксперты [Иволгин, 2021, С. 165].

Важным элементом правильности применения криминалистического подхода в этом случае является правильная постановка вопросов перед экспертом, за счет получения ответов на которые, будет понятно содержание, метод и средство совершения преступления. На этом основании будет проще установить личность преступника [Дубаев, Могилевцева, Съедина, 2021; Сёмин, Бунин, 2022].

Рассмотренные криминалистические подходы, применяемые на разных стадиях расследования преступлений в IT-сфере, дают свои результаты, но с течением времени развитие новых знаний и навыков киберпреступников приводит к необходимости внедрения в криминалистику новых подходов и направлений расследования.

Таким подходом может стать предлагаемое В. Б. Веховым и П. С. Пастуховым мнение о необходимости внедрения элементов электронной криминалистики [Вехов, Пастухов, 2018, С.138].

Данные авторы полагают, что возникшие проблемы правоприменительной деятельности борьбы с компьютерными преступлениями, необходимо решать в сфере разработки теории электронных доказательств в рамках науки уголовного процесса и установления ее науковедческих связей с электронной криминалистикой.

Наряду с технологизацией уголовно-процессуальной деятельности идет развитие практической криминалистической деятельности, внедряются новые технико-криминалистические средства: мобильный криминалист, UFED, XRY, Encase и другие аппаратно-программные комплексы, предназначенные для собирания и проверки цифровых следов преступлений.

При этом проблема остается все той же – нехватка специалистов, обладающих прикладными познаниями в IT-сфере в системе органов предварительного расследования и дознания, а также тех, кого можно привлечь в качестве специалистов и экспертов при проведении экспертизы и получения доказательств по уголовным делам.

Хорошие специалисты в IT-технологиях, особенно те, которые досконально знают методы и приемы работы киберпреступников, достаточно редки и на практике не всегда охотно участвуют в помощи органам предварительного расследования в установлении всех обстоятельств совершения преступлений.

Кроме того, проблемой является также то, что в современной криминалистике на сегодняшний день отсутствуют четкие теоретические основы и подходы, подкрепленные практическими рекомендациями к совершению последовательных тактических действий по расследованию IT-преступлений.

Те же рекомендации по криминалистике раскрытия преступления в IT-сфере, которые все же были разработаны, в скором времени устаревают в связи с применением преступниками новых способов и методов хищения имущества,

несанкционированного доступа к базам данных, незаконного использования криптовалюты для обналичивания денежных средств.

В этом контексте ориентир современной криминалистики идет на формирование единой частной теории и модели, которая объединит в себя следующие ключевые инновационные направления подходов к криминалистике расследования преступлений в сфере IT-технологий:

– использование криминалистических методов исследования IT-информации в компьютерах, программных продуктах, обработка ее специалистами в сфере IT-технологий;

– тактику осуществления необходимых следственных действий, направленных на формирование доказательной базы в электронном виде, так называемых электронных доказательств для уголовного дела;

– разработку автоматизированных методик расследования преступлений.

Сущность данного подхода состоит, прежде всего, в исследовании компьютерной информации, которое должно найти свое отражение в предлагаемой В. Б. Веховым и П. С. Пастуховым «Электронной криминалистике», которую предполагается сформировать в виде концепций и научных положений криминалистики расследования преступлений в IT-сфере, на основе которых уже будет формироваться современная система методов и приемов получения информации в ходе расследования преступлений [Вехов, Пастухов, 2018, С. 138]. Большое значение в электронной криминалистике придается именно изучению компьютерной информации, установлению факта совершения преступления, средства и метода преступления, а также непосредственно субъекта преступления. Электронная криминалистика также будет способствовать установлению объективной и субъективной стороны совершения преступления в сфере IT-технологий.

Планируется, что по своему содержанию и сущности электронная криминалистика будет столь же разносторонней и многогранной, как и система кри-

миналистических технологий и подходов в расследовании обычных классических преступлений, не связанных с IT-сферой.

Для более обстоятельного и предметного изучения в «Электронную криминалистику» предлагается включить подразделы, раскрывающие криминалистические аспекты функционирования информационно-технологических средств:

1. Криминалистическое учение о юридических, технических и гносеологических аспектах компьютерной информации.

2. Криминалистическое исследование компьютерных устройств, информационных систем и информационно-телекоммуникационных сетей.

3. Криминалистическое использование компьютерной информации деятельности по раскрытию и расследованию преступлений.

Оценивая предлагаемый подход к формированию системы электронной криминалистики, следует отметить, что в текущих условиях действительно требуется реформация существующих классических криминалистических подходов к расследованию преступлений для их применения при компьютерных преступлениях, кибермошенничестве и иных формах уголовных IT-правонарушений. Требуется именно та система, которая будет постоянно трансформироваться под изменения научно-технического прогресса, темпы развития цифровизации, которые и используются преступниками в процессе совершения преступлений в киберпространстве.

Тем самым предлагаемая электронная криминалистика имеет большое будущее в современной системе криминалистических подходов в расследовании преступлений в IT-сфере.

Библиографический список

1. Багмет А. М., Антонов О. Ю., Бычков В. В. Криминалистика. – Москва : Проспект, 2020. – 240 с.

2. Бахов К. А., Беккер А. Э. Мошенничество с использованием платежных карт. / В сборнике: Проблемы экономики и управления: социокультурные, правовые и организационные аспекты. Сборник статей магистрантов и преподавателей КузГТУ. Посвящается 300-

летию Кузбасса и 70-летию КузГТУ. Под редакцией В.М. Золотухина, В.Г. Михайлова. – Кемерово, 2020. – С. 144–149.

3. Бертовский Л. В. Криминалистика. – Москва : Проспект, 2021. – 960 с.

4. Вехов В. Б., Пастухов П.С. Преступления в информационном обществе: совершенствование расследования на основе положений электронной криминалистики. // Ex jure. – 2018. – №4. – С. 134-148. [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/prestupleniya-v-informatsionnom-obschestve-sovershenstvovanie-rassledovaniya-na-osnove-polozheniy-elektronnoy-kriminalistiki (дата обращения: 10.02.2023).

5. Гаврилов Е. О. Цифровой суверенитет в условиях глобализации: философский и правовой аспекты // Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки, 2020. – Т. 4. – № 2. – С. 146–152. DOI: https://doi.org/10.21603/2542-1840-2020-4-2-146-152.

6. Дубаев Л. А. И., Могилевцева А. А., Съедина Н. В. Уголовно-правовое значение мотива. / В сборнике: Проблемы экономики и управления: социокультурные, правовые и организационные аспекты. Сборник статей магистрантов и преподавателей КузГТУ. – Кемерово, 2021. – С. 194–199.

7. Иволгин А. К. Современная криминалистика в IT-сфере. – Москва : Юрайт, 2021. – 320 с.

8. Золотухин В. М., Золотухин М. В. Проблемы цифровой безопасности в условиях развития технологий. / Проблемы экономики и управления: социокультурные, правовые и организационные аспекты : сборник статей магистрантов и преподавателей КузГТУ (четвертый выпуск) / под ред. В. М. Золотухина, В. Г. Михайлова ; КузГТУ – Кемерово, 2022. – С. 76–84.

9. Золотухин В. М. Цифровые коммуникации и социокультурные риски в российской ментальности. / В сборнике: Социальные коммуникации: философские, политические, культурно-исторические измерения. сборник статей II Всероссийской научно-практической конференции с международным участием. – Кемерово, 2021. С. 49–54.

10. Золотухин В. М. Социальные коммуникации в рамках российской социокультурной ментальности. / В сборнике: Социальные коммуникации: философские, политические, культурно-исторические измерения. сборник статей I Всероссийской научно-практической конференции с международным участием. Кемеровский государственный университет. – Кемерово, 2020. С. 95–99.

11. Золотухин В. М., Козырева М. В. Совершение сделок малолетними гражданами в условиях современного российского правоприменения. // Теория и практика социогуманитарных наук. 2021. – № 1 (13). – С. 83–89.

12. Криминалистика / Отв. ред. Ищенко Е.П. – Москва : Проспект, 2021. – 816 с.

13. Маинов М. С. Маркетинговый комплекс IT-продукта. / В сборнике: Проблемы экономики и управления: социокультурные, правовые и организационные аспекты. Сборник статей магистрантов и преподавателей КузГТУ. Кузбасский государственный технический университет имени Т.Ф. Горбачева. – Кемерово, 2022. – С. 399–407.

14. Михайлов М. А., Кокодей Т. А. Цифровые инновации и права человека: дилеммы международной правоохранительной практики. // Правоприменение. – 2022. – Т. 6, № 3. – С. 120–133. – DOI: 10.52468/2542-1514.2022.6(2).120-133.

15. Слонов Е. А., Козырева М. В. Проблема наследования цифровых активов: социокультурный и правовой аспекты. / В сборнике: Проблемы экономики и управления: социокультурные, правовые и организационные аспекты. Сборник статей магистрантов и преподавателей КузГТУ. Кузбасский государственный технический университет имени Т.Ф. Горбачева. – Кемерово, 2022. – С. 482–491.

16. Линев П. А. Специфика маркетинговой деятельности в сфере IT-услуг В сборнике: Проблемы экономики и управления: социокультурные, правовые и организационные аспекты. Сборник статей магистрантов и преподавателей КузГТУ. Кузбасский государственный технический университет имени Т.Ф. Горбачева. – Кемерово, 2022. – С. 392–398.

17. Количенко А.А. Электронные носители информации как источник получения электронных доказательств в уголовном процессе // Вестник Казанского юридического института МВД России, 2022. – Т. 13. – № 1 (47). – С. 114–121. DOI: 10.37973/KUI.2022.69.32.016.

18. Сёмин З. И., Бунин М. Е. Проблемы идентификации и квалификации жертв преступления. / В сборнике: Проблемы экономики и управления: социокультурные, правовые и организационные аспекты. Сборник статей магистрантов и преподавателей КузГТУ. Кузбасский государственный технический университет имени Т.Ф. Горбачева. – Кемерово, 2022. – С. 273–281.

19. Третьякова И. Н. Оценка эффективности интернет-маркетинга ПАО «ВТБ» В сборнике: Конкуренция и монополия. Сборник материалов IV Всероссийской научно-практической конференции студентов, магистрантов, аспирантов, научно-педагогических работников и специалистов в области антимонопольного регулирования. Под общей редакцией Н.В. Кудреватых, В.Г. Михайлова. – Кемерово, 2021. – С. 268–273.

20. Труфанова Е., Хан Ш. Трансформации культурной идентичности в цифровую эпоху // Вопросы философии. 2022. – № 12. – С. 84–94.

21. Тюнис И. О. Криминалистика. Учебное пособие. – Москва : Проспект, 2020. – 220 с.

22. Gritskevich, T.I., Zolotukhin, V.M., Kazakov, E.F. Sociocultural Grounds for Transforming the Concept of “Man Without Essence” Smart Innovation, Systems and Technologies, 2019, 139, pp. 743–751.

23. Zolotukhin V. M., Zhukova O. I. Man and Transformation of His Socio-Cultural Values in the Ethnic-National Aspect. Smart Innovation, Systems and Technologies. 2019. Т. 139. С. 772-777.

P. A. Grevtsov, V. A. Mitkov, A. A. Moskalenko
T.F. Gorbachev Kuzbass State Technical University, Kemerovo, Russia

FORENSIC APPROACHES TO THE INVESTIGATION OF CRIMES IN THE FIELD OF IT TECHNOLOGIES

supervisor: D. F. N., Professor of history, philosophy and social Sciences Zolotukhin V. M.

The growth of cyberbullying, the creation of electronic digital signatures, hacking of personal accounts of citizens and legal entities, theft of passwords, etc. actualizes the search for methods, methods and mechanisms to combat them. In this regard, the role of the use of forensic approaches to the investigation of crimes in the field of IT technologies is increasing. It is emphasized that criminalistic approaches aimed at establishing the motive for committing a crime in the IT sphere are associated with the identification of persons possibly involved in the crime as employees of an enterprise, a bank in which crimes were committed using IT technologies or employees who had access to private data and subsequently quit.

Keywords: cyberbullying, IT technologies, confidential information, offenses, personal data.