СОВРЕМЕННОЕ СОСТОЯНИЕ И ТЕНДЕНЦИИ ДАЛЬНЕЙШЕГО РАЗВИТИЯ СИСТЕМЫ КРИМИНАЛИСТИЧЕСКОГО ОБЕСПЕЧЕНИЯ БОРЬБЫ С ПРЕСТУПНОСТЬЮ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СФЕРЕ

Каримов В.Х., Каримов А.В.
Алтайский государственный университет, г. Барнаул
e-mail: karimovvh@mail.ru

Аннотация. В статье исследуются проблемы криминалистического обеспечения борьбы с преступлениями, с использованием современных технологий, в частности с применением информационно-телекоммуникационных систем. Уделено внимание вопросам применения средств и методов раскрытия и расследования преступлений, которые основаны на цифровых технологиях. Проведен анализ нового, активно развивающего направления – цифровой криминалистики. Выявлены закономерности развития цифровой криминалистики, формирование научных взглядов в данной области, как в России, так и зарубежных странах. Обозначаются пробелы нормативно-правового регулирования рассматриваемой сферы и необходимость разработки новых криминалистических подходов в борьбе с преступлениями с внедрением современных информационных технологий, отвечающих реалиям времени. Сказанное обуславливает потребность в разработке соответствующих тактико и технико-криминалистических средств и методов. В работе проведен анализ существующей системы борьбы с преступлениями в информационной сфере. Изучена научная разработанность вопросов, посвященных применению криминалистических средств и методов в борьбе с киберпреступностью. Предложены основные направления совершенствования данной системы. В частности, по мнению авторов, необходим анализ существующего состояния государственной политики по предупреждению и борьбе с преступлениями информационно-телекоммуникационной сфере, включая сеть Интернет, определение количественных и качественных характеристик механизма рассматриваемых преступлений, изучение личности киберпреступника, исследование существующих информационных сетей и технологий, используемых преступниками для совершения преступлений, в том числе, использующих возможности шифрования и анонимизации данных пользователей и другое.

Ключевые слова: Криминалистическое обеспечение, компьютерные преступления, киберпреступник, информационные технологии, информационно-поисковые системы, цифровая криминалистика.

Произошедшая в XX веке новая волна технологической революции, обусловленная появлением компьютерной техники, развитием информационно-телекоммуникационной среды и сети Интернет привела к созданию постиндустриального, цифрового общества. Произошли качественные преобразования всех сфер человеческой жизнедеятельности и не только позитивные, такие как улучшение качества жизни, увеличение производительности труда и т.д., но и негативные, обусловленные активным использованием информационно-цифровых технологий в криминальных целях. В частности, сеть Интернет, становится огромным рынком нелегальной продукции, средством общения преступников, через нее совершается ряд мошенничеств, преступлений экономической направленности, деяния террористического и экстремистского характера, имеется угроза и национальной безопасности.

Так, по данным международной службы по обеспечению безопасности в области киберугроз Symatec Security каждую секунду кибератаке подвергается 12

человек, ежегодно в мире совершается 556 млн. преступлений, ущерб от которых составляет более 100 млрд. дол. США [1, с. 46]. Указанные проблемы не могут не отражаться и в официальных статистических данных. При общем снижении зарегистрированных преступлений, число уголовных деяний с использованием высокотехнологичных способов продолжало неуклонно расти.

При этом статистические данные не отражают в полной мере тех угроз, которые исходят из информационно-телекоммуникационной среды, поскольку такие преступления обладают высокой латентностью. Так, по данным Судебного департамента РФ за первое полугодие 2019 года в России за преступления, включенные в Главу 28 УК РФ (Преступления в сфере компьютерной информации) осуждено всего 79 лиц, что, безусловно, не отражает реального положения дел. Некоторые криминальные проявления статистикой вовсе не учитываются. Например, явные признаки принадлежности к деструктивному, распространяемому через Интернет движению «Колумбайн» у В. Рослякова, совершившего массовое убийство в Керченском политехническом колледже в октябре 2018 года: (оружие, место, способ совершения преступления, одежда, в которую был одет убийца), следствием учтены не были, и, соответственно, никто из популяризаторов таких идей ответственности не понес. Аналогичным способом было совершенно и совсем недавнее убийство в ноябре 2019 года в одном из колледжей г. Благовещенска, где жертвами стрелка стал один человек, еще трое получили ранения, сам нападающий застрелился.

Государство, осознавая очевидность угроз, исходящих из информационно-цифровой среды, в последние годы ведет определенную политику, отражаемую, в частности в «Стратегии развития информационного общества в Российской Федерации на 2017-2030 гг.». За последние несколько лет, ряд преступных деяний, с использованием информационно-телекоммуникационных сетей были признаны общественно-опасными и включены либо в диспозиции статей, либо в их квалифицированные признаки: например, в статьи: 110, 110.1,151.2, 158, 159,3, 171.2, 185.3, 250.2, 228,1, 242.1, 272-274.1, 282 УК РФ. Но одной криминализации деяний, по нашему мнению, явно не достаточно. Необходимо эффективно предупреждать, выявлять, раскрывать и расследовать подобные деяния, в том числе с помощью криминалистических средств и методов. В настоящее время, современные информационные технологии стремительно развиваются, а отечественная юридическая наука, законотворчество и правоприменительная практика, обладая свойством стабильности, а по сути - статичности, оказались не готовыми на должном уровне противостоять рассматриваемым криминальным явлениям.

Сказанное обуславливает необходимость разработки и совершенствования системы криминалистического обеспечения по предупреждению, раскрытию и расследованию преступлений в информационно-телекоммуникационной сфере.

В целом, анализ научных источников, посвященных криминалистическим аспектам борьбы с преступлениями в информационно-телекоммуникационной сфере, показывает на изученность отдельных направлений данной сферы. Так, общие вопросы криминалистического обеспечения доказывания по уголовным делам и общие положениям методики расследования компьютерных преступлений были рассмотрены в докторских диссертациях: Новика В. В., Волынского А.Ф., Мещерякова В.А. [2, 3, 4]. Вопросы использования правоохранительными органами информационно-поисковых систем в раскрытии и расследовании преступлений рассмотрены в работах Каримова В.Х., Кравец Е.Г. [5, 6]. Понятие содержание компьютерной информации в криминалистике уделено внимание в трудах Вехова В.Б. [7]. Расследованиям отдельных видов преступлений, совершаемых в сети Интернет, посвящены работы: Атаманова Р.С., Коломинова В.В., Ильюшина Д.А. [8,

9, 10]. Проблемам расследования компьютерных преступлений уделено внимания в диссертациях: Полякова В.В., Костомарова К.В. [11, 12]. Имеется также достаточное количество публикаций по отдельным вопросам рассматриваемой темы.

Анализ научных работ, посвященных криминалистическому обеспечению в информационно-цифровой сфере в зарубежных странах, показал, что к началу XXI века была сформирована новая область исследований – изучение киберпреступности, которая включала не только криминалистические, но криминологические, уголовно-правовые и процессуальные аспекты борьбы с ней.

При этом на начало нулевых годов XXI века, изучению данной сферы были посвящены лишь отдельные публикации. Между тем, развитие компьютерных и информационных технологий развивалось столь стремительно, что образовался правовой, методический и технический вакуум в обеспечении борьбы с данными криминальными проявлениями, чем не могла не воспользоваться преступная среда. Потребовались усилия всего международного сообщества в принятии соответствующих адекватных решений.

Так, в марте 2001 года в Будапеште была подписана Конвенция Совета Европы ETS № 185 (Конвенция о преступности в сфере компьютерной информации). Она открыта не только для стран Европы, но других государств мира [13]. Например, ее подписали США и Япония. Данная Конвенция обозначила и нормативно закрепила понятие киберпреступности, подразделив преступления в киберпространстве на четыре основные группы:

- против конфиденциальности, целостности и доступности компьютерных данных и систем;
- преступные деяния, направленные на использование компьютерных средств и технологий;
- преступления, связанные с производством, распространение через компьютерную сеть детской порнографии, а также ее хранением в компьютерных системах;
- преступления, посягающие на авторские и смежные права;
- преступления, связанные распространение через компьютерную сеть информации экстремистского характера.

К сожалению, Россия не подписала рассматриваемую Конвенцию, что в безусловной мере ограничивает потенциал не только нашей страны, но и других государств в международной борьбе с преступления в информационно-телекоммуникационной сфере. Полагаем, что такой документ должен быть подписан.

Рассматривая дальнейшее развитие системы криминалистического обеспечения по борьбе с киберпреступностью, отметим, что к ^{кон}цу первого десятилетия XXI века исследования в рассматриваемой области стали системными и детальными. Между тем, авторы работ не отошли от сложившего на тот момент подхода, включив в нее не только вопросы криминалистического обеспечения, например, изъятия цифровой информации, проведение киберрасследований, цифровую криминалистику и анализ данных, но и процедуру подготовки к судебному преследованию и даче показаний, а также криминологические аспекты по предупреждению киберпреступности.

Безусловно, рассмотрение киберпреступности в таком виде было явно не достаточно для разработки и проведения криминалистических исследований, направленных на расследование преступлений в информационно-телекоммуникационной сфере. В дальнейших работах, мы можем наблюдать большее внимание именно криминалистическим аспектам борьбы. Так, с начала 10-х годов XXI века в научной литературе прочно вошел в обиход термин, обозначающий, по сути, развитие новой и перспективной сферы – Цифровой криминалистики. В частности, сказанное отражается в работах: «Киберпреступность

и цифровая криминалистика: введение», Д. Томаса, А. Босслера, С. Кэтрина., «Основы цифровой криминалистики. Теория, методы и реальные приложения» К. Иоакима [14, 15].

На необходимость развития цифровой криминалистики обращается в научных публикациях и российских ученных. Так, Комаров И.М., отмечет, что "Цифровая" криминалистика это давно назревшая проблема, без чего практическая правоприменительная деятельность в современных условиях уже эффективно не реализуется» [16, с.161.]. Аналогичного мнения придерживается Яковлев А.Н., указывающий, что: «Обращать на данную проблему необходимо сейчас, поскольку завтра будет уже поздно» [17]. В.А. Мещеряков, определяет место специальным познаниям в цифровой криминалистике [18, с. 87-92]. Скобелин С.Ю., акцентирует внимание на электронных следах преступлений [19, с. 178-181], Федотов Н.Н., развивает новое направление компьютерной криминалистики – форензику [20].

Следует заметить, несмотря на то, что расследование киберпреступлений и цифровая криминалистика имеют схожую, а во многом общую основу криминалистической деятельности, объекты их исследований полностью не совпадают, поскольку помимо изучения преступлений в киберпространстве и исследования электронно-цифровых следов, криминалистическое обеспечение в информационно-телекоммуникационной сфере имеет и более широкие задачи – применения информационных сетей в целях при расследовании общеуголовных преступлений. Например, для розыска убийцы по социальным сетям и т.д.

Таким образом, проведенный выше анализ позволил нам сделать следующие выводы.

Полагаем, имеющие пробелы криминалистического обеспечения в информационно-телекоммуникационной сфере носят системный характер и обусловлены следующими причинами:

1) в праве не выработано единого понимания преступлений, в информационно-телекоммуникационной сфере, они разбросаны по множеству составов;

2) в криминалистической науке не проведены системные исследования проблемных вопросов криминалистического обеспечения в информационно-телекоммуникационной среде и её применения для решения задач по раскрытию, расследованию и предупреждению преступлений. Имеющие наработки носят частный характер и посвящены отдельным аспектам данной проблемы. Причины, по нашему мнению, заключаются в том, что традиционно, методики расследования преступлений отдельных видов соотносятся с конкретными статьями и главами Уголовного кодекса РФ. Между тем, расследование отдельных составов, зачастую обладает предельной обобщенностью и расплывчатостью, отсутствием конкретизации криминалистических задач, устаревшим характером таких алгоритмов [21, с. 62]. К примеру, в составе уголовного деяния, предусмотренного статьей 110.1 УК РФ (Склонение к совершению самоубийства или содействие совершению самоубийства), способы совершения, связанные с использованием с информационно-телекоммуникационных сетей (включая сеть "Интернет") будут существенно отличаться от других, что потребует особых подходов к методике расследования. С другой стороны, у разных составов преступлений, где используется информационно-телекоммуникационные сети много общего с точки зрения способа и механизма совершения преступлений, личности преступника, средств, используемых для совершения таких преступлений, что позволяет разрабатывать общие рекомендации, которых на сегодняшний момент нет;

3) имеется сложность в применении традиционных криминалистических методов, средств, приемов, методик, поскольку они не становятся эффективны.

Таким образом, в настоящее время, в отечественной науке не проведено системных исследований, посвященных вопросам криминалистического обеспечения в информационно-телекоммуникационной сфере. Смежные вопросы «Цифровой» криминалистики находятся на стадии обозначения проблемы и научной дискуссии.

Полагаем, научные исследования по заявленной теме должны быть проведены по следующим направлениям:

1. анализу существующего состояния реализации государственной политики по предупреждению и борьбе с преступлениями информационно-телекоммуникационной сфере, включая сеть Интернет;
2. определение количественных и качественных характеристик механизма рассматриваемых преступлений;
3. изучение личности киберпреступника;
4. исследование существующих информационных сетей и технологий, используемых преступниками для совершения преступлений, в том числе, использующих возможности шифрования и анонимизации данных пользователей;
5. изучение возможных способов противодействия расследованию преступлений в сфере информационно-телекоммуникационных технологий и предложение путей их преодоления;
6. разработка рекомендаций по использованию информационно-телекоммуникационных сетей для розыска лиц скрывшихся от суда и следствия, установления пропавших без вести, раскрытия и расследования общеуголовных преступлений;
7. разработка использования криминалистических технологий направленных на решение социальных задач (например, по воспитание молодежи через ограничение деструктивного контента в сети Интернет, выявленного при расследовании преступлений, розыск пропавших лиц с помощью криминалистических информационных технологий через социальные сети др.);
8. построение теоретической модели системы криминалистического обеспечения и практического механизма борьбы с преступлениями в информационно-телекоммуникационной сфере, включая сеть Интернет, построенной на исследованиях в области права, информатики, социологии, психологии;
9. разработка основ методик раскрытия и расследования преступлений в информационно-телекоммуникационных сфере;
10. внедрение в практику предложений по профилактике, раскрытию и расследованию рассматриваемых преступлений.

Библиографический список

1. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть, 2014. - № 8. – С. 46-48.
2. Новик В. В. Криминалистическое обеспечение, доказывания по уголовным делам: проблемы теории и практики: дисс…докт. юрид. наук. - Москва, 2009. – 642 с.
3. Волынский А.Ф. Концептуальные основы технико-криминалистического обеспечения раскрытия и расследования преступлений: дисс…докт. юрид. наук. - Москва, 1999. – 65 с.
4. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: дисс… докт. юрид. наук. - Воронеж, 2001. - 387 с.
5. Каримов В.Х. Современное состояние и перспективы развития информационно-поисковых систем криминалистического назначения: дисс… канд. юрид. наук. - Москва, 2012. – 213 с.

6. Кравец Е.Г. Информационно-коммуникационные технологии как элемент технико-криминалистического обеспечения расследования преступлений: дисс… канд. юрид. наук. - Волгоград, 2016. – 208 с.
7. Вехов В.Б. Криминалистическое учение о компьютерной информации и средствах ее обработки: дисс…докт. юрид. наук. - Волгоград, 2008. – 561 с.
8. Атаманов Р.С. Основы методики расследования мошенничества в сети Интернет: дисс… канд. юрид. наук. - Москва, 2012. – 182 с.
9. Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дисс… канд. юрид. наук. Краснодар, 2017. – 177 с.
10. Ильюшин Д.А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: дисс… канд. юрид. наук. - Волгоград, 2008. – 233 с.
11. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: дисс… канд. юрид. наук. - Омск, 2008. – 244 с.
12. Костомаров К.В. Первоначальный этап расследования преступлений, связанных с незаконным доступом к компьютерной информации банков. дисс… канд. юрид. наук. - Екатеринбург, 2012. – 212 с.
13. Convention on Cybercrime Details of Treaty №185.
14. Thomas, J., Bossler, M., Kathryn, C., Seigfried-Spellar Cybercrime and Digital Forensics: An Introduction, Routledge: 2nd ed, Berlin, Heidelberg. 2017.
15. Joakim, K., (2018), Fundamentals of Digital Forensics. Theory, Methods, and Real-Life Applications, Springer International Publishing, Berlin, Heidelberg.
16. Комаров И.М. «Цифровая» криминалистика - давно назревшая проблема. // Библиотека криминалиста. Научный журнал, 2018. – 2 (37). – С.161-171.
17. Яковлев А.Н. Цифровая криминалистика как фактор защиты цифровой экономики. // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) [Электронный ресурс] : сборник статей Международной научно-практической конференции. – Электронные текстовые данные (2,33 Мб). – М.: Академия управления МВД России, 2018.
18. Мещеряков В.А. Особенности специальных знаний, используемых в цифровой криминалистике // Известия Тульского государственного университета. Экономические и юридические науки, 2013. -Т 4-2. - С. 87-92.
19. Скобелин С.Ю. Цифровая криминалистика: понятие, возможности, перспективы // Труды Академии МВД Республики Таджикистан. Материалы республиканской научно-практической конференции с участием международных экспертов "Роль криминалистики в раскрытии и расследовании преступлений" (Душанбе, 25 сентября 2015 г.). - С. 178-181.
20. Федотов Н.Н. Форензика – компьютерная криминалистика – М.: Юридический Мир, 2007. – 432 с.
21. Долгинов С.Д. Информационное обеспечение следственной деятельности: возможности и реальность // Труды Академии МВД Республики Таджикистан, 2018.- № 2 (38). – С. 58-69.

CURRENT STATE AND TENDENCIES FOR FURTHER DEVELOPMENT OF THE CRIMINALISTIC SUPPORT SYSTEM FOR COMBATING CRIME IN THE INFORMATION AND TELECOMMUNICATION SPHERE

Karimov V.Kh., Karimov A.V.
Altai State University, Barnaul
email: karimovvh@mail.ru

Abstract. The article examines the problems of forensic support of the fight against crimes, using modern technologies, in particular with the use of information and telecommunication systems. Attention is paid to the issues of using means and methods of disclosing and investigating crimes that are based on digital technologies. The analysis of a new, actively developing area - digital forensics. The patterns of development of digital forensics, the formation of scientific views in this area, both in Russia and foreign countries, have been identified. The gaps in the legal regulation of the area under consideration and the need to develop new forensic approaches in the fight against crimes with the introduction of modern information technologies that meet the realities of the time are indicated. The foregoing determines the need for the development of appropriate tactical and technical-forensic tools and methods. The paper analyzes the existing system of combating crimes in the information sphere. The scientific elaboration of issues on the use of forensic tools and methods in the fight against cybercrime has been studied. The main directions for improving this system are proposed. In particular, according to the authors, it is necessary to analyze the existing state of the state policy on preventing and combating crimes in the information and telecommunications sphere, including the Internet, determining the quantitative and qualitative characteristics of the mechanism of the crimes in question, studying the personality of a cybercriminal, researching existing information networks and technologies used by criminals. to commit crimes, including those using the encryption and anonymization of user data, and more.

Keywords: Forensic support, computer crime, cybercriminal, information technology, information retrieval systems, digital forensics.