РАЗДЕЛ 3
ТРАНСФОРМАЦИЯ ПРАВА В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ

КРИМИНАЛИСТИЧЕСКИЕ ТЕХНОЛОГИИ РАБОТЫ СО СЛЕДАМИ КИБЕРПЕРСТУПЛЕНИЙ

Т.Ф. Дмитриева

Ключевые слова: киберпреступность, криминалистические технологии, следы, компьютерные средства, расследование преступлений.

Характерной чертой современного информационного общества является проникновение информационных технологий практически во все сферы жизни. Криминальные проявления с использованием компьютерных, банковских и других электронных средств оказывают дестабилизирующее воздействие на общество, обуславливают потребность в создании эффективного механизма противодействия киберпреступности, укрепления правопорядка, обеспечения защиты личности, прав и свобод граждан, повышения их доверия к структурам власти и управления. Проблема повышения эффективности криминалистического обеспечения борьбы с киберпреступностью является одной из актуальных проблем криминалистики, поскольку расследование таких преступлений представляет нелегкую задачу установления механизма совершения противоправного деяния по ограниченному числу признаков, требующую значительных усилий, профессионализма, проницательности, наблюдательности, логики мышления. Общеизвестно, что существенный рост киберпреступности фиксируется практически во всех странах. При расследовании киберпреступлений особую важность приобретает эффективное применение специальных знаний и криминалистических технологий, отвечающих современному уровню развития науки и техники, обеспечивающих полноту обнаружения, фиксации и изъятия специфических следов преступления и иных материальных объектов. Сказанное свидетельствует об актуальности выбранной автором темы исследования.

Проблемам использования средств криминалистической техники посвящены работы М.Б. Вандера, Е.И. Гончаренко, Г.И. Грамовича, В.И. Громова, Е.П. Ищенко, А.А. Леви, П.В. Макалинского, С.М. Потапова, Р.А. Рейсса, С.Н. Трегубова, А.А. Эйсмана и др. Криминалистические и процессуальные вопросы применения новых (компьютерных и цифровых) технологий при расследовании преступлений нашли свое отражение в работах Е.Н. Дмитриева, О.Б. Дроновой, С.Б. Коваленко, Д.В. Муленкова и др. Возможности применения компьютерных технологий при осмотре места

происшествия исследовали В.Е. Козлов, Э.А. Ли и др.; криминалистических технологий – Ф.Г. Аминев, цифровых – В.А. Газизов, Л.М. Исаева и др. Изучение литературы свидетельствует о том, что проведенные ранее исследования имеют большое теоретическое и практическое значение. Однако многие работы отражают лишь отдельные аспекты применения достижений науки и техники в расследовании преступлений. За пределами научного осмысления остались теоретические и прикладные проблемы применения современных криминалистических технологий при расследовании преступлений вообще и киберпреступлений – в частности. Данные обстоятельства указывают на необходимость комплексного подхода к решению указанных проблем.

Понятие «киберпреступность», хотя и утвердилось в последние десятилетия в качестве как доктринального, так и правового термина, тем не менее, в русскоязычной литературе это понятие чаще всего используется в качестве синонима термина «компьютерная преступность» или «преступления в сфере компьютерной информации». В Республике Беларусь, термин «киберпреступность» хотя и используется – примером может служить его применение в Гл.19 Концепции информационной безопасности Республики Беларусь от 18 марта 2019 г., тем не менее правового определения не имеет. В белорусском уголовном законодательстве применяется понятие «преступления против информационной безопасности» [1, Гл. 31]. Объединяющими признаками всех преступлений, входящих в состав киберпреступности, являются средства их совершения – киберпространство, информационно-телекоммуникационные сети и средства компьютерной техники. Соответственно, киберпреступность можно определить как «совокупность противоправных деяний, совершаемых с использованием информационно-коммуникационных технологий (ИКТ) и либо нацеленных на сети, системы, данные, веб-сайты и/или технологии, либо способствующих совершению преступления» [2, p. 440].

Современный уровень развития цифровых криминалистических технологий расследования преступлений делает возможным, с одной стороны, существенное снижение латентности преступности, с другой – значительное повышение коэффициента раскрываемости преступлений, причем это относится как к традиционной уголовной преступности, так и к рассматриваемой в данной работе киберпреступности. Между тем, в проблемном поле криминалистики находится ряд актуальных дискуссионных аспектов, существенно влияющих на процесс раскрытия, расследования и предупреждения киберпреступлений, среди которых разработка адекватных современной криминогенной ситуации технико-криминалистических подходов к расследованию киберпреступлений, обновление учеными-криминалистами методик расследования компьютерных преступлений в современных условиях, совершенствование структуры методики расследований киберпреступлений, позволяющей поднять борьбу с киберпреступностью на соответствующий уровень.

В числе характерных признаков криминалистической характеристики преступлений в сфере компьютерной информации ученые выделяют следы совершения преступления (виртуальные либо материальные) [3]. Следы – важное средство установления объективной истины по делу, поэтому работа с материальными следами на месте происшествия – исходный и наиболее важный момент расследования преступлений. Собирание доказательств – это понятие комплексное, включающее действия по обнаружению, фиксации, изъятию и сохранению следов преступления. Эффективность деятельности по выявлению (обнаружению) следов киберпреступлений зависит от компетенции и профессионализма лица, реализующего технологии их применения в каждом конкретном случае осмотра места происшествия. На практике имеются недостатки применения криминалистических технологий при расследовании преступлений [4, с.134]. Тем не менее, криминалистические технологии обнаружения, фиксации, изъятия и сохранения следов киберпреступлений могут открыть самый короткий путь к установлению лица, совершившего преступление. От результативности их применения при осмотре места происшествия зависит не только эффективность данного следственного действия, но и увеличение объема доказательственной информации, необходимой для расследования киберпреступления.

Под криминалистическими технологиями осмотра места происшествия нами понимается «непрерывный процесс использования субъектами его криминалистического обеспечения комплекса современных технико-криминалистических средств; целесообразных, эффективных способов и методов, тактико-криминалистических приемов их применения в должной последовательности, в условиях дефицита времени, необходимости решения значительного числа сложных мыслительных задач при крайней недостаточности информации о событии преступления в целях получения максимально полной и необходимой информации по расследуемому преступному событию, от применения которого зависит эффективность следственного действия и расследования в целом» [4, с.118].

Базируясь на ранее предложенной нами систематизации криминалистических технологий осмотра места происшествия [4, с.118], считаем целесообразным выделить систему криминалистических технологий работы со следами киберпреступлений. Так, на первом уровне криминалистические технологии работы со следами киберпреступлений в зависимости от выполняемых с помощью технико-криминалистических средств функций могут быть подразделены на следующие группы: 1) криминалистическая технология выявления (обнаружения) следов киберпреступления; 2) криминалистическая технология фиксации следов; 3) криминалистическая технология изъятия следов. На втором уровне для систематизации криминалистических технологий киберпреступления основанием могут служить объекты, для выявления (обнаружения) которых используются технико-криминалистические средства. По этому основанию целесообразно выделить 6 групп

криминалистических технологий выявления (обнаружения), поиска: 1) аудио-, видеозаписей или фотоизображений; 2) неметаллических следов и объектов (компьютерных, электронных и др.); 3) следов папиллярных узоров; 4) микрообъектов; 5) металлических предметов; 6) комплекса следов. При такой систематизации, на наш взгляд, можно обеспечить результативность, полноту и качество выявления (обнаружения) всего комплекса разнообразных следов, позволяющих обеспечить эффективность расследования киберпреступления.

Так, например, обнаружение аудио-, видео- или фотоизображений является важным действием формирования доказательственной совокупности. В криминалистической структуре киберпреступления элементом материальной обстановки места его совершения могут служить электронные приборы с функцией памяти (телефонные аппараты, смартфоны, планшеты и иные), обладающие свойством сохранять в электронной памяти вводимую владельцем информацию личного характера, а также сведения об обстоятельствах их эксплуатации. По своим сущностным характеристикам данная информация аналогична сведениям, которые обрабатывается компьютерами, она недоступна для непосредственного восприятия без специального аппаратного и программного обеспечения, легко изменяется, передается по сетям связи. При осмотре места происшествия можно обнаружить объекты, содержащие уголовно релевантные записи, созданные различными электронными цифровыми средствами, к которым относятся цифровые регистраторы речи и камеры видеонаблюдения (том числе различные web-камеры), а также мобильные телефоны, системы IP- и Интернет-телефонии и иные средства пакетной передачи оцифрованной речи. Изображения, зафиксированные камерой видеонаблюдения, дают объективную информацию о внешности преступника и требуют применение необходимого компьютерного оборудования для ее просмотра и фиксации. Комплекс технических средств управления информационными ресурсами представляет собой электрические, электронные, электромеханические технические средства, используемые для хранения, обработки, передачи информации, в состав которых входят компьютеры и их периферия, а также средства и каналы связи [4, с.157].

Представляется, что предложенные криминалистические технологии работы со следами киберпреступлений будут способствовать получению качественно более полной и содержательной информации о преступнике, механизме совершения противоправного деяния и достижению целей и задач данной деятельности в каждом конкретном случае.

Список использованных источников:

1. Уголовный кодекс Республики Беларусь: принят Палатой представителей 2 июня 1999 года: одобрен Советом Республики 24 июня 1999 года // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Республики Беларусь. – Минск, 2021.

2. Maras, Marie-Helen. Cybercriminology. Oxford University Press, USA, 2016. – 448 p.

3. Степаненко, Д.А. Цифровая реальность и криминалистика / Д.А. Степаненко, В.В. Коломинов // ГлаголЪ правосудия. – 2018. – № 3 (17). – С. 38–43.

4. Дмитриева, Т.Ф. Криминалистическое обеспечение осмотра места происшествия: монография / Т.Ф. Дмитриева; под науч. ред. Е.И. Климовой. – Витебск: ВГУ имени П.М. Машерова», 2016. – 307 с.

ЦИФРОВИЗАЦИЯ ПРАВА НА СОВРЕМЕННОМ ЭТАПЕ: РИСКИ И ВОЗМОЖНОСТИ

Д.А. Кавецкий

Ключевые слова: искусственный интеллект, робот, сервисное государство, цифровое право, цифровая экономика, электронное государство, электронное лицо.

В век цифровых технологий существует угроза распространения недостоверной информации. «Потоки недостоверной, а порой и откровенно лживой информации уже давно захлестнули практически все источники массового распространения новостного контента. Дошло до того, что Министерство Иностранных дел России открыло на своем официальном сайте специальный раздел, где представлены публикации, распространяющие недостоверные новости о Российской Федерации» [1, с.12].

Между гражданином и государством должна быть обратная связь. Это одна из задач «электронного государства». «Применительно к электронным технологиям это означает необходимость создания электронной почты, сайтов, страниц в социальных сетях для государственных и муниципальных органов власти и управления с соответствующими возможностями для обратной связи» [2, с.60].

Фейковые новости стали угрозой для интернет-демократии.

Нужно различать такие понятия как «информатизация судов» и «электронное правосудие». В «информатизации судов» компьютерные технологии используются как средства. «В качестве примеров электронного правосудия можно привести такие, как подача исков, регистрация заявлений, представление отзывов на иски в электронном виде, электронное судебное дело, движение этого дела из суда в суд в электронной форме, заседания с помощью видео-конференций и.д.» [3, с.145-146].

Кто должен нести юридическую ответственность при передаче медицинской диагностики искусственному интеллекту – если произошла ошибка в постановке диагноза? Если диагноз будет ставить робот? В данном случае