взрывчатых веществ проводятся и другие виды криминалистических экспертиз, которые зависят от конкретной ситуации и специфики обнаруженных следов.

Библиографический список

1. Габа, А. И. Современные возможности криминалистического исследования веществ, материалов и изделий из них: практ. пособие / А. И. Габа, Д. В. Исютин-Федотков. – Минск: РИВШ, 2009. – 146 с.

2. Подготовка и назначение судебных экспертиз: пособие для следователей, судей и экспертов / А. С. Рубис [и др.]; отв. ред. А. С. Рубис. – Минск: Харвест, 2006. – 320 с.

3. Мухин, Г. Н. Криминалистическая дерматоглифика: моногр. / Г. Н. Мухин, О. Г. Каразей, Д. В. Исютин-Федотков. – Минск: Акад. МВД Респ. Беларусь, 2006. – 91 с.

4. Пацкевич, А. П. Использование дактилоскопической информации в выявлении, расследовании и предупреждении преступлений: моногр. / А. П. Пацкевич, С. Н. Сороженко. – Минск: Акад. МВД, 2011. – 115 с.

СОВРЕМЕННЫЕ ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ ЦИФРОВОЙ КРИМИНАЛИСТИКИ

Талалаев В. А., Лемешевский О. О.

УО «Военная академия Республики Беларусь»,
ул. Уручская, 1а, 220056,Минск, Беларусь, varb@mod.mil.by

Криминалистика на сегодняшний день развивается в условиях цифровизации и информатизации. Закономерности, входящие в предмет криминалистики, подвергаются изменению под воздействием сложившихся обстоятельств. В публикации приведены отдельные аспекты места, роли и современных характеристик криминалистического исследования цифровой информации. Авторами делается акцент на проблематике изучаемой области, которая включает в себя понимание о том, что современная теоретическая база по исследованию цифровизации с точки зрения криминалистики является разноплановой и требует дальнейшего изучения. В этой связи определяется необходимость разработки новых методов взаимодействия с информацией в цифровом мире. Уточняются направления разработки приемов для решения различных криминалистических задач в цифровом пространстве.

Ключевые слова: цифровая криминалистика; интернет; компьютерные технологии; виртуальный мир; расследование; киберпреступность; месседжеры

Современный этап развития нашего общества ознаменован бурным развитием компьютерных технологий, цифровых устройств, сети интернет. Повсеместная компьютеризация общественных отношений отразилась на преступности и способах противодействия этому явлению. Следуя современным трендам, преступный элемент использует «виртуальный мир» как площадку для подготовки, совершения и сокрытия противоправных деяний, различных видов и групп.

По отдельным данным в городе Минске в 2022 году около 99% населения в возрасте от 6 до 72 лет пользовались услугами сотовой связи; 95.2% – использо-

вали сеть Интернет, более 80,5% – пользовались персональным компьютером и данные показатели продолжают неуклонно расти.

Следует отметить, что все процессы, происходящие в «виртуальном» мире, оставляют большое количество следов таких, как:

– пассивные (техническая информация использования электронных устройств);

– активные (следы действий, совершенных непосредственным пользователем: фотографии, видео, различные записи).

Обнаружением и фиксацией таких следов занимается относительно новая отрасль криминалистики – цифровая криминалистика [1, с. 11].

За последние пять лет количество киберпреступлений выросло в десяток раз. В этой связи вопрос их профилактики и пресечения остается актуальным, так как удельный вес таких деяний в структуре преступности остается значительным (более 16%).

Важным является положение о том, что на данном этапе происходит процесс совершенствования подобного вида преступлений, к примеру:

– в интернете продавцы наркотиков формируют так называемые службы безопасности из подростков, желающих заработать «легкие деньги». В их «задачи» входит возвращение долгов у провинившихся наркокурьеров. Следует отметить, что данных молодых людей в последующем могут использовать для совершения преступлений, в том числе экстремисткой направленности;

– совершенствуются способы совершения и сокрытия киберпреступлений для дестабилизации общественно-политической обстановки, нанесения ущерба государственным органам и организациям;

– следует ожидать дальнейшего совершенствования способов хищений путем использования компьютерной техники, случаев несанкционированного доступа к компьютерной информации, совершаемых, в частности посредством фишинга, взлома учетных записей пользователей в социальных сетях и др.

На основе изучения способов совершения перечисленных выше преступлений, можно констатировать, что они совершаются в двух мирах, один из которых – привычный нам мир материальных объектов, а другой – виртуальный. К примеру, используя карты накопления бонусных баллов в магазинах, также используем сеть интернет как источник получения информации, разнообразное программное обеспечение как инструмент для социальных связей, социальные сети «ВКонтакте», «Фейсбук» и др., инструмент для общения (мессенджеры WhatsApp, Telegram и т.п.), инструмент для решения профессиональных задач (офисные программы с поддержкой облачного хранения информации и другие). Современные устройства, используемых человеком, от мобильных телефонов до смарт-телевизоров также хранят на своих носителях и во внешних хранилищах информации следы использования человеком.

Изучением применения и совершенствования подходов расследования преступлений в современных реалиях информационного общества занимается цифровая криминалистика – относительно новый термин, который уже является устоявшимся. Вместе с тем, сложившаяся ситуация требует, как можно быстрее

пройти путь научного становления этого направления и перейти к практической реализации ее положений при расследовании преступлений.

Новые знания ориентированы на понимание функционирования информационно-коммуникационных технологий и выявления различных закономерностей:

преступной деятельности, направленной на воспрепятствование нормальному функционированию информационных систем, их компонентов или деятельности, направленной на использование последних в качестве инструмента совершения иных преступлений, к примеру: взлом страниц общественной организации «Белорусский республиканский союз молодежи», атаки на интернет каналы и сайты государственных средств массовой информации, атаки на сайты государственных органов и т.д.

создания, изменения, передачи, удаления информации на электронных носителях, в информационно-телекоммуникационных сетях, виртуальном пространстве, связанной с подготовкой, совершением, сокрытием преступлений, ярким примером будет, являться: инструктажи преступных элементов через экстремистские телеграмм каналы о приобретении специального программного обеспечения, способствующего очищению памяти телефона в случае опасности для преступника.

формирования цифровой информации, сохраненной в отдельных информационных объектах, а также в информационной среде электронного носителя информации, представляющей собой: фотографии и видеозаписи, сохраняющиеся параллельно с памятью мобильного телефона на «облачных» хранилищах в сети интернет такие, как Google Foto, Google Disk;

интеграции цифровых сведений в систему существующих доказательств с соблюдением процессуальной формы их получения: внедрение в правовую базу Республики Беларусь определения цифровых доказательств [2, с. 40].

Здесь отметим различия во мнениях о том, каким термином обозначить доказательства, которые хранятся в электронном виде, в том числе на электронных носителях и в сети Интернет, и нет единого подхода об определении сущности данной информации в уголовно-процессуальном контексте.

В рамках теории цифровой криминалистики предполагается рассматривать тактику отдельных процессуальных действий в цифровой среде, элементы аппаратно-программного обеспечения научной организации труда следователя и информационного обеспечения, программные комплексы, направленные на содействие следствию в построении версий, планировании расследования и иных организационных мероприятиях. Ведь ведущую роль в цифровой криминалистике, играет именно специализированное программное обеспечение (ПО) и широта его возможностей, а не специалист или эксперт, – проще сказать, не человек. Объясняется это тем, что сложность и многослойность цифровых устройств, их технические характеристики, а также действия преступников в цифровом пространстве настолько ускорены и усовершенствованы возможностями этого пространства, что человеческий мозг не в силах противостоять им в одиночку.

Здесь также следует отметить развивающиеся способности искусственного интеллекта и специализированные сайты по указанному направлению (типа GPT).

Придерживаясь данного положения, следует отметить, что в силу географического положения, ассортимент наркотиков в Республике Беларусь достаточно обширный. Наш подход в борьбе с наркотиками таков, что в стране запрещены 98% известных в мире психоактивных веществ. Когда-то в законодательстве были введены понятия «аналоги» и «базовые структуры». Если специалистами выявляется новое психоактивное вещество, которое имеет аналоги в списке уже запрещенных, то в течение короткого времени оно вносится в список запрещенных или контролируемых в обороте. Более того, у нас запрещены даже те вещества, которые даже на рынке не появились, но известно, что у соседей они есть. Такой белорусский опыт перенимают Россия, Казахстан, другие государства.

Практика свидетельствует, что подавляющее большинство клиентов продавцов наркотиков в интернете не в состоянии понять, как попасть в «даркнет» и разобраться с биткоином, другими видами криптовалют. Аудитория, употребляющая и распространяющая наркотики, пользуется телеграм-каналами и телеграм-чатами, посвященными специфике такой деятельности. Реклама таких магазинов распространяется через граффити в различных местах.

С учетом тематики, представляется интересным работа по поиску и задержанию лиц, распространяющих наркотики через интернет. Сотрудники представляются заинтересованными клиентами, располагая преступника к общению, и просят пройти по гиперссылке содержащей предмет разговора. В случае перехода получается информация, содержащая IP-адрес лица, перешедшего по ссылке, а также данные об используемой им операционной системе, браузере, языках, часовом поясе, а при определенных обстоятельствах – даже о модели мобильного телефона. Подобные этому инструменты также позволяют получать данные об аккаунте социальных сетей, электронной почте с последующей идентификацией и задержанием причастных лиц.

Одним из основных способов противодействия использованию информационно – коммуникационных технологий в преступных целях может стать обучение сотрудников правоохранительных органов использованию специального программного обеспечения.

Перспективу для решения данной проблемы открывает автоматизированный компьютерный продукт в виде комплекса криминалистических материалов по применению технологий расследования преступлений в сфере интернет-преступности. Вместе с тем, необходимо продолжить разработку частных криминалистических методик расследования преступлений в сфере информационно-коммуникационной безопасности.

Таким образом, цифровую криминалистику на современном этапе представляют как сложную систему, совокупность программ для исследования цифрового пространства с целью профилактики, выявления и пресечения преступлений, анализа цифрового материала, носителей цифровых материалов для обнаружения, изъятия и фиксации преступления.

Библиографический список

1. Цифровая криминалистика: учебник для вузов / В. Б. Вехов [и др.] ; под ред. В. Б. Вехова, С. В. Зуева. – Москва : Издательство Юрайт, 2021. – 417 с.

2. Уголовно-правовые, криминологические и криминалистические проблемы расследования и предупреждения киберпреступлений для специальности II ступени высшего образования (магистратура): учебно-методический комплекс по учебной дисциплине / сост.: Т. Ф. Дмитриева, В. Г. Стаценко. – Витебск : ВГУ имени П.М. Машерова, 2022. – 83 с.

ИСПОЛЬЗОВАНИЕ ГИПНОЗА ПРИ ОПРОСЕ

Титов П. М.

ФГКУ ВО «Уральский юридический институт МВД России»
ул. Корепина, 66, 620057, г. Екатеринбург, Россия, strikegun@mail.ru

В статье рассматривается вопрос об использовании гипноза при осуществлении опроса. Делается упор на законодательное применение гипноза на основе Российского права. Анализируются точки зрения ученых. В работе также исследуются особенности применения специальных знаний – гипноза при опросе в ходе раскрытия и расследования преступлений. При написании статьи использовались общенаучные и частнонаучные методы. В заключении даются рекомендации по применению гипноза в практической деятельности правоохранительных органов.

Ключевые слова: криминалистика; оперативно-розыскная деятельность; специальные знания; преступления; опрос

Федеральный закон Российской Федерации «Об оперативно-розыскной деятельности» [1] закрепил в ст. 6 перечень оперативно-розыскных мероприятий, однако, определения, что такое оперативно-розыскные мероприятия не закрепил. В научной литературе имеются множество определений оперативно-розыскных мероприятий, однако хотелось бы выделить определение, которое дают П.М. Титов и В.Ю. Стальмах: «Оперативно-розыскные мероприятия – это предусмотренные Федеральным законом «Об оперативно-розыскной деятельности» познавательные действия (совокупность действий), производимые уполномоченными сотрудниками оперативно-розыскных органов, при наличии фактических и юридических оснований, для реализации целей оперативно-розыскной деятельности гласными, негласными или зашифрованными способами, частично обеспеченные мерами государственного принуждения, ход и результаты которых документируются в установленном порядке» [2, с. 45-46]. На наш взгляд, данное определение наиболее четко отражает суть оперативно-розыскных мероприятий.

Переходя к первому оперативно-розыскному мероприятию, хотелось бы обратить внимание на то, что в настоящее время существует несколько разновидностей способов проведения оперативно-розыскного мероприятия − «опрос». Классификация включает в себя гласные и негласные способы, легендированный и зашифрованный опрос.