данного вида преступлений объектом поиска выступает информация, отражающая направленность умысла на приобретение или сбыт наркотиков, как, например, непосредственно переписка приобретателя со сбытчиком, номера телефонов, паспортные и иные данные для совершения денежных переводов, иная информация, распространяемая через интернет, характеризующая преступную направленность. В свою очередь, объект и особенности информационно-аналитической деятельности автором раскрыты фрагментарно и не являются исчерпывающими, но при этом имеют прикладное значение при выявлении наркопреступлений.

Таким образом, в настоящее время отсутствует единый подход к пониманию понятия информационно-аналитической деятельности при выявлении преступлений, в том числе наркопреступлений, совершаемых в сети Интернет.

Ряд вопросов информационно-аналитической деятельности при выявлении наркопреступлений требуют научной проработки, наиболее актуальными для комплексного исследования являются аспекты, связанные с определением сущности, содержания, особенностей информационно-аналитической деятельности; получения информации и анализа ее источников, используемых при ее осуществлении; связанные с информационно-аналитическим и тактическим обеспечением данной деятельности.

УДК 343.98

О.П. Виноградова

ТАКТИКО-КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ПРОВЕДЕНИЯ НЕВЕРБАЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Преступления в сфере информационно-телекоммуникационных технологий с каждым годом приобретают все большее распространение. Это связано с ростом уровня информатизации общества и внедрения интернет-технологий, что напрямую способствует увеличению таких преступлений, как кражи, совершенные с помощью интернет-технологий. В России на начало этого года насчитывалось 129,8 млн интернет-пользователей [1]. На рост пользователей сети Интернет, несомненно, повлияла пандемия коронавирусной инфекции COVID-19. Распространение коронавирусной инфекции повлияло на работу многих офлайн-площадок по продаже различных товаров и услуг и, следовательно, увеличилось количество интернет-магазинов. Все это, наряду с «цифровым невежеством» [2], обусловило значительное увеличение количества киберпреступлений.

В то же время, несмотря на понижение темпа роста рассматриваемых преступлений, нельзя не отметить, что кражи, совершенные с помощью интернет-технологий, и в целом все киберпреступления постоянно со временем видоизменяются и совершенствуются, что снижает эффективность по их выявлению, раскрытию и расследованию. Развитие преступной среды предопределяет возможность обезличивания злоумышленников, а также совершение таких преступлений дистанционно, что позволяет скрыть следы. В связи с этим растет уровень совершаемых рассматриваемых преступлений, поэтому деятельность правоохранительных органов в настоящее время направлена на выявление, раскрытие и расследование краж, совершенных с использованием интернет-технологий.

Лицам, проводящим осмотр, необходимо знать, что компьютерно-техническое устройство находится в выключенном состоянии, его необходимо оставить в этом состоянии, чтобы предотвратить потерю доказательственной информации, а если устройство было включено, то стоит обратить внимание на информацию, содержащуюся на экране, об уровне заряда устройства, об операционной системе, службе доступа к файлам и сети. В данной ситуации могут быть выявлены цифровые следы преступления. Как отмечают В.О. Давыдов и И.В. Тишутина, такие цифровые следы «имеют высокую скорость трансформации, легко уничтожаются и модифицируются, могут быть представлены бесконечным количеством копий, легко распространяются в компьютерных сетях и доступны в любой точке, где имеется подключение к сети Интернет, цифровой или электронный след может состоять из большого количества отдельных информационных элементов, которые могут быть записаны как на одном, так и на нескольких электронных носителях информации, подключенных как к одному, так и к нескольким компьютерам, объединенным в информационную систему или информационно-телекоммуникационную сеть» [3]. Стоит отметить также, что на устройстве, которое является объектом осмотра, может быть установлена защита, требующая ввода определенного защитного кода или другой специальной команды, и если не произвести вышеперечисленные действия, то информация на устройстве может быть уничтожена, и поэтому для получения доступа к осматриваемому устройству необходим пароль. В таком случае считается целесообразным получить указанные пароли добровольно. Если будут проведены все эти действия, то обнаружение и копирование значимой информации для расследования уголовного дела будет осуществлено в более короткий

срок. В противном случае, несоблюдение порядка этих действий может привести к утере информации, содержащейся на компьютерно-техническом устройстве. Копирование информации с объекта осмотра осуществляется с возможностью сохранения неизменности копируемой информации с применением накопителей большой вместимости, для того чтобы в процессе копирования необходимые данные не были утрачены. Сохранность и неизменность изъятых следов на месте происшествия достигаются использованием надлежащих упаковочных материалов, исключающих возможность их физического повреждения.

Обыск по данной категории уголовных дел обладает определенной спецификой и требует незамедлительного проведения после возбуждения уголовного дела, поскольку следы преступления могут быть утрачены.

При подготовке к обыску должностное лицо должно определить следующие аспекты.

Выбрать оптимальный день и время для производства обыска. Если обыск проводится в жилом помещении, стоит выбрать то время, когда владельцы находятся дома, в служебных помещениях обыск проводится в рабочее время.

Провести анализ имеющейся информации о месте производства обыска (вид жилого помещения, количество этажей, расположение комнат, наличие в комнатах компьютерной техники и др.), также об обыскиваемых лицах и лицах, которые могут находиться в месте, где производится обыск, о наличии домашних животных, о путях подхода и отхода.

Исходя из анализа вышеуказанной информации, определяется состав участников следственного действия, решается вопрос о привлечении специалиста в области информационных технологий.

Определение необходимых технических средств, необходимых для производства следственного действия, а также предметов, которые нужны для изъятия и упаковки следов преступления.

Изъятие мобильного устройства и планшета обладает специфическими особенностями, потому что помимо электронной информации эти устройства несут в себе материальные следы, свидетельствующие о том, что именно подозреваемый пользовался данным устройством, например, следы пальцев рук, микрочастицы и т. д. Для упаковки и изъятия следов преступления обязательно привлекается специалист. При изъятии мобильный телефон переводится в режим полета. Изымать следует с зарядным устройством, это относится не только к мобильному устройству, а также и к ноутбуку.

На заключительном этапе составляется протокол следственного действия, в котором фиксируются абсолютно все проводимые действия, например, нажатие на клавиши, место обнаружения устройства и др., к протоколу прилагаются чертежи и схемы.

Список использованных источников

1. Global Digital 2022: вышел ежегодный отчет об интернете и социальных сетях – главные цифры [Электронный ресурс]. – URL: https://www.sostav.ru/publication/we-are-social-i-hootsuite-52472 (дата обращения: 20.10.2022).

2. Пандемия и цифровое невежество: эксперты назвали причины роста киберпреступности в России [Электронный ресурс]. – URL: https://online47-ru.turbopages.org/ (дата обращения: 23.10.2022).

3. Давыдов, В.О. Цифровые следы в расследовании дистанционного мошенничества / В.О. Давыдов // Изв. Тул. гос. ун-та. экон. и юрид. науки. – 2020. – № 3. – С. 22.

УДК 343.3

В.Р. Гайнельзянова

О ПОДГОТОВИТЕЛЬНОМ ЭТАПЕ ОСМОТРА МЕСТА ПРОИСШЕСТВИЯ В ХОДЕ РАССЛЕДОВАНИЯ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Борьба с преступлениями, связанными с неправомерным доступом к компьютерной информации, в современных реалиях становится одной из приоритетных задач правоохранительных органов. Часто у лиц, производящих действия в пределах своей компетенции, в рамках расследования возникают определенные сложности в получении сведений о месте, времени и других данных, которые характеризуют совершенное деяние. Извлечение же криминалистически значимой информации об обстоятельствах преступления относится к числу важнейших составляющих работы следователя. Процесс получения таких данных осуществляется путем реализации осмотра места происшествия.

Расширение использования информационно-телекоммуникационных технологий во всем мире привело к правовым проблемам. Неблагоприятным условием процесса цифровизации общества являются компьютерные преступления, представляющие реальную угрозу не только для отдельных пользователей электронно-вычислительных машин, но и в целом для национальной безопасности страны.

Сохраняется высокая латентность данного вида преступления, которая обусловлена недостаточной цифровой грамотностью граждан, распространением программных средств анонимизации личности, обеспечивающих сокрытие информации о совершившем преступление лице, размножением программ для мобильных устройств, позволяющих перехватывать сетевой трафик, расшифровывать имена и пароли пользователей и пр. При этом следует констатировать низкую эффективность про-