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-

изводства предварительного следствия по преступлениям в сфере компьютерной информации и судебного рассмотрения таких дел.

Указанный вид преступлений относится к группе сложных в расследовании и идентификации лиц, их совершивших. Использование преступниками возможностей информационно-телекоммуникационных технологий затрудняет определение механизма преступления, вследствие чего усложняется реализация следственных действий.

Приведем пример из правоприменительной практики. Так, Р.С.И. совершил неправомерный доступ к компьютерной информации, в результате которого осуществил списание со счета личных кабинетов интернет-магазина Sitilink бонусных баллов в виде денежных средств на сумму 31 776 р., принадлежащих С.Р.Т. По результатам проверки несанкционированных действий Р.С.И. произошла модификация компьютерной информации, выразившаяся в изменении количества бонусных денежных средств, которые принадлежали правообладателям личных кабинетов вышеуказанного интернет-магазина, а также преобразование их контактной информации и блокирование доступа к личным данным кабинета интернет-магазина.

В практике расследования неправомерного доступа к компьютерной информации осмотр места происшествия является первоначальным неотложным следственным действием, результаты которого представляются главными составляющими в сборе доказательственной базы.

Неправомерный доступ к компьютерной информации реализуется с использованием цифровых технологий и ресурсов сети Интернет. В связи с этим место совершения несанкционированных действий становится не конкретно-определенным. Криминалистически значимая информация, интересующая предварительное следствие, может находиться и в иных местах, а именно: в местах размещения цифровых носителей с данными, полученными в результате преступного деяния; в местах нахождения цифровых носителей со сведениями, которые могут представлять интерес для следствия; в местах, где установлены общественно опасные последствия от несанкционированных действий.

Перед проведением данного следственного действия с особой бдительностью и достаточной ответственностью рекомендуется подходить к избранию специалиста.

Основной целью осмотра места происшествия по уголовным делам указанного вида является установление определенного ЭВМ и компьютерных сведений, которые могут выражаться в качестве предмета либо орудия, используемых в реализации преступных действий, и содержать объекты преступной деятельности.

В ходе подготовительного этапа к осмотру места происшествия по делам о неправомерном доступе к компьютерной информации у руководителя учреждения, а также лица, отвечающего за обслуживание и

использование компьютерного оборудования, либо иного сотрудника предприятия, фирмы, следует взять объяснение, а при возбуждении уголовного дела – допросить и выяснить обстоятельства, связанные с блокированием помещения, где находится вычислительная техника, электронная система либо оборудование охранной сигнализации, разрешения, также логины, пароли, коды, дополнительные устройства и документация для беспрепятственного доступа к ним. Следует помнить, что дистанционное блокирование помещения связано с механизмом самоуничтожения значимой информации в компьютерном оборудовании, действие которой определяется вмонтированным в ЭВМ источником питания. При несоблюдении правил входа в помещение включается устройство защиты и ЭВМ устраняет значимую информацию на винчестере. Организации, эксплуатирующие данные механизмы уничтожения важных сведений на жестком диске вычислительной техники, часто имеют скрытую систему резервирования данных.

Алгоритм действий следственно-оперативной группы по прибытию на место происшествия, в первую очередь, путем криминалистических приемов фотографирования, рекомендуется зафиксировать сложившуюся обстановку на месте происшествия. Специалисту в данной отрасли знаний предлагается выполнить мероприятия, направленные на недопущение воздействия на имеющуюся информацию. Для этого путем отстранения их от компьютерных средств необходимо лишить сотрудников организации возможности выполнять действия по осуществлению порчи сведений, размещая их в ином помещении, по возможности изъять у них средства вычислительной техники. От услуг специалистов организации в сфере компьютерной информации целесообразно отказаться во избежание повреждения (уничтожения) информации.

Исходя из вышеизложенного, подытожим, что эффективность производства осмотра места происшествия при расследовании указанного вида преступлений обусловлена организацией тщательной подготовки к осмотру места происшествия, непременным использованием специальных познаний в области информационно-телекоммуникационных технологий и, соответственно, привлечением лиц, обладающих знаниями, опытом работы в данной сфере. В целях установления обстоятельств совершения неправомерного доступа к компьютерной информации совместная работа следователя и специалиста может осуществляться как на этапе получения консультативной информации, так и в ходе реализации рабочего этапа осмотра места происшествия. Решающее значение в ходе производства данного следственного действия имеет правильная фиксация и изъятие, упаковка объектов преступления, которые требуют обоснованного информационного взаимодействия следователя и специалиста.