Учреждение образования
«Академия Министерства внутренних дел Республики Беларусь»

ОРГАНИЗАЦИЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Рекомендовано Министерством внутренних дел Республики Беларусь
в качестве учебного пособия
для обучающихся учреждений высшего образования
Министерства внутренних дел Республики Беларусь

Под общей редакцией
кандидата юридических наук И.Г. Мухина

Минск
Академия МВД
2017

УДК 343.985.7
ББК 67.52
О-64

Авторы:

П.В. Гридюшко (разд. 5, 6, 8), А.Н. Лепёхин (разд. 7),
И.Г. Мухин (разд. 1–3, 5, 6), Д.В. Петко (разд. 5),
И.А. Судникович (разд. 3, 4), А.Е. Сушко (разд. 3, 5, 6), Ю.М. Юбко (разд. 4, 8)

Рецензенты:

Следственный комитет Республики Беларусь;
кафедра государственно-правовых дисциплин факультета права
Белорусского государственного экономического университета;
заместитель директора ГУ «Научно-практический центр проблем укрепления
законности и правопорядка» Генеральной прокуратуры Республики Беларусь
доктор юридических наук, доцент *А.Е. Гучок*

О-64 **Организация расследования преступлений в сфере высоких технологий** : учебное пособие / П.В. Гридюшко [и др.] ; под общ. ред. И.Г. Мухина ; учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь». – Минск : Академия МВД, 2017. – 139, [1] с.

ISBN 978-985-576-030-7.

Рассматриваются современные проблемы борьбы с противоправными деяниями, относящимися к преступлениям в сфере высоких технологий. Раскрываются основы деятельности следователя по расследованию таких преступлений, рекомендации по проведению отдельных следственных действий.

Предназначено для лиц, обучающихся в учреждениях образования Министерства внутренних дел Республики Беларусь, профессорско-преподавательского состава указанных учреждений образования, сотрудников правоохранительных органов.

УДК 343.985.7
ББК 67.52

ISBN 978-985-576-030-7

1. ПРЕДМЕТ, ЗАДАЧИ И СИСТЕМА УЧЕБНОЙ ДИСЦИПЛИНЫ «ОРГАНИЗАЦИЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ»

Предметом любой науки является определенная группа объективных закономерностей действительности, которые отражаются данной наукой и образуют сферу познания именно этой, а не какой-либо другой области знания.

Организация расследования преступлений в сфере высоких технологий – специальная учебная дисциплина, изучающая закономерности механизма совершения преступлений указанной категории, возникновения информации о таких преступлениях и их участниках, обнаружения, фиксации, исследования и использования доказательств по делам о данных преступлениях, а также специальные средства и методы расследования преступлений в сфере высоких технологий, основанные на познании этих закономерностей.

Предмет рассматриваемой учебной дисциплины составляют:

– закономерности механизма совершения преступления указанной категории;

– закономерности возникновения информации о данных преступлениях и их участниках, связанные с закономерностями возникновения следовой информации по делам рассматриваемой категории;

– закономерности обнаружения, фиксации, исследования и использования доказательств.

Целью изучения учебной дисциплины «Организация расследования преступлений в сфере высоких технологий» является приобретение теоретических знаний с учетом конкретных, динамично развивающихся ситуаций при производстве по уголовным делам указанной категории; формирование умений и привитие навыков самостоятельного выполнения функциональных обязанностей следователя, правильной оценки реальной обстановки в ходе производства по материалам и уголовным

делам данной категории и принятия необходимых организационных, процессуальных и тактических решений.

Предмет и цель учебной дисциплины определили ее следующие ***задачи***:

– изучение уголовно-правовых, уголовно-процессуальных и тактических особенностей расследования преступлений в сфере высоких технологий;

– обучение комплексному использованию теоретических знаний основных юридических наук в процессе расследования преступлений данной категории;

– формирование умений и выработка навыков законного и обоснованного производства следственных и иных процессуальных действий;

– выработка установки на недопустимость нарушения действующего законодательства Республики Беларусь при производстве по материалам и уголовным делам данной категории;

– формирование умений и выработка навыков документального оформления хода и результатов следственных и иных процессуальных действий, а также принятия организационных, процессуальных и тактических решений по уголовным делам о преступлениях в сфере высоких технологий.

Учебная дисциплина «Организация расследования преступлений в сфере высоких технологий» раскрывает информационные и методические основы расследования преступлений рассматриваемой группы.

К информационным основам относятся понятие организации расследования преступлений в сфере высоких технологий, сущность компьютерной преступности, виды компьютерных преступлений и типы преступников, современное состояние борьбы с киберпреступностью и др.

К методическим основам относятся особенности возбуждения уголовных дел о преступлениях в сфере высоких технологий, тактика осмотра средств компьютерной техники и компьютерной информации, методика расследования отдельных видов преступлений.

Таким образом, ***система*** данной учебной дисциплины включает совокупность знаний из научных областей криминалистики, криминологии, уголовного права, уголовного процесса и оперативно-розыскной деятельности, т. е. обладает синтетическим характером. Изучаемая дисциплина тесно связана прежде всего с наукой криминалистикой, в одном из разделов которой изучается система частных криминалистических методик, в том числе и методика расследования преступлений в сфере высоких технологий, а также с теорией оперативно-розыскной деятельности органов внутренних дел, изучающей проблемы выявления и раскрытия преступлений рассматриваемой группы. Указанная учебная дисциплина состоит из следующих разделов:

– характеристики преступлений в сфере высоких технологий;

– обстоятельств, подлежащих доказыванию, и иных элементов информационных основ расследования преступлений в сфере высоких технологий;

– типичных следственных ситуаций, возникающих в процессе расследования преступлений в сфере высоких технологий;

– действий следователя на первоначальном этапе расследования преступлений в сфере высоких технологий, особенностей возбуждения уголовного дела по делам рассматриваемой категории;

– тактики использования специальных знаний в процессе расследования преступлений в сфере высоких технологий (в том числе назначения компьютерно-технических экспертиз);

– причин совершения преступлений в сфере высоких технологий и условий, им способствующих.

Изучение характеристики преступлений в сфере высоких технологий предполагает уяснение следующих проблемных вопросов:

– что подразумевается под компьютерной преступностью в международных нормативных правовых актах;

– какие составы преступлений, относящихся к преступлениям в сфере высоких технологий, предусмотрены действующим Уголовным кодексом Республики Беларусь (далее – УК);

– кто и какими способами совершает эти преступления.

Категория «компьютерные преступления» является собирательной. К числу компьютерных преступлений относятся как преступления в сфере компьютерной информации либо ее защиты, так и преступления, совершаемые с использованием компьютерных технологий.

Соответственно, **компьютерная преступность** – количественная и качественная совокупность уголовно наказуемых деяний, направленных против охраняемых законом интересов человека, общества, государства, совершенных в сфере компьютерной информации либо ее защиты, а также в сфере использования средств компьютерной техники в целях достижения преступного результата.

Собирательность данной категории обусловливается следующими факторами: *по субъектам* предупреждения, выявления, пресечения и раскрытия такая деятельность, как правило, осуществляется специализированными подразделениями по противодействию высокотехнологичной, либо компьютерной, преступности; *по методам*, используемым для осуществления противодействия, – специальные оперативно-технические и оперативно-аналитические мероприятия, проводимые для предупреждения, выявления, пресечения и раскрытия преступлений данной группы; *по решаемым задачам* в процессе осуществления противодействия компьютерной преступности; *по используемым средствам деятельности* – специализированным программным, аппарат-

ным и аппаратно-программным модулям (арсенал специальных технических и программных средств).

В современной литературе, посвященной проблемам компьютерной преступности, существуют следующие ***классификации преступлений в сфере высоких технологий***.

Первая классификация:

1) преступления против информационной безопасности (гл. 31 УК: несанкционированный доступ к компьютерной информации (ст. 349); модификация компьютерной информации (ст. 350); компьютерный саботаж (ст. 351); неправомерное завладение компьютерной информацией (ст. 352); изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 353); разработка, использование либо распространение вредоносных программ (ст. 354); нарушение правил эксплуатации компьютерной системы или сети (ст. 355));

2) хищения путем использования средств компьютерной техники (ст. 212 УК);

3) изготовление и распространение порнографических материалов или предметов порнографического характера (ст. 343 УК); изготовление и распространение порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего (ст. 343^1 УК);

4) иные преступления, так или иначе связанные с использованием компьютерной техники (например, доведение до самоубийства (ст. 145 УК) путем систематического унижения личного достоинства (распространения каких-либо сведений в сети Интернет); разглашение врачебной тайны (ст. 178 УК); незаконное собирание либо распространение информации о частной жизни (ст. 179 УК); незаконные действия, направленные на трудоустройство граждан за границей (ст. 187 УК); клевета (ст. 188 УК); оскорбление (ст. 189); нарушение авторского права, смежных прав и права промышленной собственности (ст. 201 УК); нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений (ст. 203 УК); изготовление, хранение либо сбыт поддельных денег или ценных бумаг (ст. 221 УК); дискредитация деловой репутации конкурента (ст. 249 УК); распространение ложной информации о товарах и услугах (ст. 250 УК); коммерческий шпионаж (ст. 254 УК); разглашение коммерческой тайны (ст. 255 УК); заведомо ложное сообщение об опасности (ст. 340 УК); шпионаж (ст. 358 УК); клевета в отношении Президента Республики Беларусь (ст. 367 УК); умышленное либо по неосторожности разглашение государственной тайны (ст. 373, 374 УК); умышленное разглашение служебной тайны (ст. 375 УК); подделка, изготовление, использование либо сбыт поддельных документов, штампов, печатей, бланков (ст. 380 УК)).

Вторая классификация:

1) противоправные деяния, при совершении которых средства компьютерной техники выступают как орудия совершения преступления;

2) противоправные деяния, при совершении которых средства компьютерной техники выступают как предмет преступного посягательства;

3) противоправные деяния, так или иначе связанные с использованием средств компьютерной техники.

Таким образом, преступления в сфере высоких технологий охватывают значительную часть УК. Однако при изучении данной учебной дисциплины невозможно охватить такое количество составов, поэтому мы остановимся только на наиболее распространенных и наиболее специфичных из них, в частности:

– преступлениях против информационной безопасности (гл. 31 УК);

– хищениях путем использования компьютерной техники (а именно с использованием банковских платежных карточек и их реквизитов (ст. 212 УК);

– распространении порнографических материалов с использованием средств компьютерной техники (ст. 343 и 343^1 УК);

– нарушении авторского права, смежных прав и права промышленной собственности (ст. 201 УК).

Преступники используют разнообразные способы получения несанкционированного доступа к компьютерной информации и постоянно изобретают новые. В силу специфики работы как самих средств компьютерной техники, так и программного обеспечения каждое такое преступление, по сути, уникально, так как различные компьютерные системы и программные комплексы их защиты работают по-разному, следовательно, и способы совершения атак на такие системы различны. Кроме того, способы совершения компьютерных преступлений зависят от квалификации злоумышленника и арсенала имеющихся у него средств.

Все ***способы совершения компьютерных преступлений*** классифицируют на четыре основные группы. При этом в качестве основного классифицирующего признака выступает метод использования преступником тех или иных действий, направленных на получение доступа к средствам компьютерной техники с различными намерениями. Руководствуясь этим признаком, выделяют следующие общие группы:

1) изъятие средств компьютерной техники;

2) перехват информации;

3) несанкционированный доступ к средствам компьютерной техники;

4) комплексные методы.

К первой группе относятся традиционные способы совершения обычных видов (некомпьютерных) преступлений, в которых действия преступника направлены на изъятие чужого имущества. Характерной отличительной чертой данной группы способов совершения компьютер-

ных преступлений является тот факт, что в них средства компьютерной техники всегда выступают только в качестве предмета преступного посягательства, а в качестве орудия совершения преступления используются иные инструменты, технические устройства и приспособления (или без их использования), не являющиеся средствами компьютерной техники.

Ко второй группе относятся способы совершения компьютерных преступлений, основанные на действиях преступника, направленных на получение данных и машинной информации посредством использования методов аудиовизуального и электромагнитного перехвата.

В этой и последующих группах преступлений средства компьютерной техники выступают в качестве как предмета, так и орудия совершения преступного посягательства.

Непосредственный (активный) перехват осуществляют с помощью непосредственного подключения к телекоммуникационному оборудованию компьютера, компьютерной системы или сети, например линии принтера или телефонному проводу канала связи, используемых для передачи данных и управляющих сигналов компьютерной техники, либо непосредственно через соответствующий порт персонального компьютера.

При *электромагнитном (пассивном) перехвате* данные и информацию перехватывают не только в канале связи, но и в помещениях, в которых находятся средства коммуникации, а также на значительном удалении от них. Так, без прямого контакта можно зафиксировать и закрепить на физический носитель электромагнитное излучение, возникающее при функционировании многих средств компьютерной техники, включая и средства коммуникации. Это физическое явление привлекает особо пристальное внимание специалистов различных профессий из-за все более широкого применения компьютерных систем обработки данных. Работа всех без исключения электронных устройств сопровождается электромагнитным излучением, в результате чего в различных электронных приемных устройствах возникают нежелательные помехи.

Аудиоперехват, или снятие информации по виброакустическому каналу, является наиболее опасным и достаточно распространенным способом совершения преступлений указанной категории. Защита от утечки информации по этому каналу очень сложна.

Видеоперехват заключается в действиях преступника, направленных на получение требуемых данных и информации путем использования различной видеооптической техники (в том числе и специальной). С ее помощью преступник получает, а в некоторых случаях и фиксирует требуемую информацию и данные, которые «снимаются» дистанционно с устройств видеоотображения, бумажных носителей информации (листинги, распечатки и т. д.), с нажимаемых клавиатурных клавиш при работе оператора (пользователя), а также с окружающих предметов и строительных конструкций.

«Уборка мусора» – этот способ совершения преступления заключается в неправомочном использовании преступником технологических отходов информационного процесса, оставленных пользователем после работы со средствами компьютерной техники. Он осуществляется в двух формах – физической и электронной.

В первом случае поиск отходов сводится к внимательному осмотру содержимого мусорных корзин, баков, емкостей для технологических отходов и сбору оставленных или выброшенных физических носителей информации.

Электронный вариант требует просмотра, а иногда и последующего исследования данных, находящихся в памяти компьютера. Он основан на некоторых технологических особенностях функционирования средств компьютерной техники. Например, последние записанные данные не всегда стираются в оперативной памяти компьютерной системы после завершения работы, или же преступник записывает только небольшую часть своей информации при законном доступе, а затем считывает предыдущие записи, выбирая нужные ему сведения.

К третьей группе способов совершения компьютерных преступлений относятся действия преступника, направленные на получение несанкционированного доступа к средствам компьютерной техники. К ним относятся нижеследующие.

«За дураком» – этот способ часто используется преступниками для проникновения в запретные зоны – как производственные помещения, так и электронные системы. Он заключается в следующем: держа в руках предметы, связанные с работой на средствах компьютерной техники (элементы маскировки), нужно ожидать кого-либо, имеющего санкционированный доступ, возле запертой двери, за которой находится предмет посягательства. Когда появляется законный пользователь, остается только войти внутрь вместе с ним или, например, попросить его помочь донести якобы необходимые для работы на компьютере предметы. Этот вариант способа рассчитан на низкую бдительность сотрудников организации и лиц, ее охраняющих. При этом преступниками может быть использован прием легендирования.

На таком же принципе основан и электронный вариант несанкционированного доступа. В этом случае он используется преступником из числа внутренних пользователей путем подключения компьютерного терминала к каналу связи через коммуникационную аппаратуру (обычно используются шлейфы, изготовленные кустарным способом, либо внутренняя телефонная проводка) в тот момент времени, когда сотрудник, отвечающий за работу средства компьютерной техники, выбранного в качестве предмета посягательства, кратковременно покидает свое рабочее место, оставляя терминал или персональный компьютер в активном режиме.

«За хвост» – этот способ съема информации заключается в следующем: преступник подключается к линии связи законного пользователя (с использованием средств компьютерной техники) и дожидается сигнала, обозначающего конец работы, перехватывает его «на себя», а потом, когда законный пользователь заканчивает активный режим, осуществляет доступ к системе.

«Компьютерный абордаж» осуществляется преступником путем случайного подбора (или заранее добытого) абонентного номера компьютерной системы потерпевшей стороны с использованием, например, обычного телефонного аппарата. После успешного соединения с вызываемым абонентом и появления в головном телефоне преступника специфического позывного сигнала, свидетельствующего о наличии модемного входа (выхода) на вызываемом абонентном номере, преступником осуществляется механическое подключение собственного модема и персонального компьютера, используемых в качестве орудия совершения преступления, к каналу телефонной связи.

При *неспешном выборе* преступник осуществляет несанкционированный доступ к компьютерной системе путем нахождения слабых мест в ее защите. Однажды обнаружив их, он может не спеша исследовать содержащуюся в системе информацию, скопировать ее на свой физический носитель и, возвращаясь к ней много раз, выбрать наиболее оптимальный предмет посягательства.

«Брешь» – при данном способе преступником осуществляется конкретизация уязвимых мест в защите компьютерной системы: определяются участки, имеющие ошибку (ошибки) или неудачную логику программного строения. Выявленные таким образом «бреши» могут использоваться преступником многократно, пока не будут обнаружены.

«Маскарад» – данный способ состоит в том, что преступник проникает в компьютерную систему, выдавая себя за законного пользователя.

Комплексные способы основаны на использовании двух или более способов, указанных в других группах.

Механизм образования следов – специфическая конкретная форма протекания процесса, конечная фаза которого представляет собой образование следа-отражения. Элементами этого механизма являются объекты следообразования – следообразующий, следовоспринимающий и вещество следа, а также следовой контакт как результат взаимодействия между ними в связи с приложением энергии к объектам следообразования.

Формами представления компьютерной информации на различных этапах ее существования в средствах компьютерной техники являются:

– отображаемая – компьютерная информация доступна для восприятия человеком непосредственно в виде символов, графики, звука;

– неотображаемая логическая – компьютерная информация представлена логическими структурами данных;

– неотображаемая физическая – компьютерная информация представлена физическими структурами – электромагнитным полем, а также проводниковыми, полупроводниковыми, магнитными, магнитооптическими и оптическими носителями.

Субъект (человек) воздействует на компьютерную информацию, которая находится в форме, доступной восприятию человеком, далее компьютерная информация преобразуется в цифровую форму, доступную для обработки программными средствами, после чего компьютерная информация преобразуется в электромагнитный сигнал, который может быть обработан аппаратными средствами компьютерной техники (вычисления, запись на носитель и т. д.).

Таким образом, сущность ***механизма следообразования*** следующая:

1) в процессе следообразования при совершении компьютерного преступления участвуют два взаимодействующих объекта: компьютер (средство компьютерной техники) в качестве следообразующего объекта, компьютерная информация – следовоспринимающего;

2) сущность данного процесса заключается в опосредованном воздействии человека через соответствующее средство деятельности – средство компьютерной техники – на материальный объект – компьютерную информацию;

3) подвергшись воздействию, компьютерная информация изменяет свои свойства (часть свойств), что и является результатом процесса отражения.

Соответственно, факторами, влияющими на процесс образования следов компьютерного преступления, являются:

– качественные характеристики компьютерной информации;

– характеристики и свойства средства компьютерной техники, которые используются объектом информатизации;

– форма представления компьютерной информации, делающая ее доступной для восприятия, с одной стороны, человеком, с другой – аппаратно-программными средствами компьютерной техники;

– формы воздействий на процессы обработки, передачи и хранения компьютерной информации;

– форма представления компьютерной информации в процессе вычислений и на носителях.

Вся работа следователя по изучению способов совершения преступления, иных признаков преследует важную и очевидную цель – выдвижение обоснованных версий о личности преступника.

Типы преступников, совершающих уголовно наказуемые деяния в сфере высоких технологий, также условно подразделены на группы.

К первой группе компьютерных преступников относятся лица, отличительной особенностью которых является устойчивое *сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности*. Эти субъекты воспринимают средства компьютерной техники как своеобразный вызов их творческим и профессиональным знаниям, умениям и навыкам. Именно это и является в социально-психологическом плане побуждающим фактором для совершения различных деяний, большинство из которых имеют ярко выраженный преступный характер. Под воздействием указанного выше фактора лицами рассматриваемой группы изобретаются различные способы несанкционированного проникновения в компьютерные системы, нередко сопровождающиеся преодолением постоянно усложняющихся средств защиты данных, что в свою очередь приводит к наращиванию алгоритма преступных действий и объективно способствует увеличению разнообразия способов совершения компьютерных преступлений. Характерной особенностью преступников этой группы является отсутствие у них четко выраженных противоправных намерений. Практически все действия они совершают с целью проявления своих интеллектуальных и профессиональных способностей. Ситуация здесь условно сравнима с той, которая возникает при различного рода играх, стимулирующих умственную активность игроков, например при игре в шахматы. В роли одного игрока выступает гипотетический преступник, а в роли его соперника – обобщенный образ компьютерной системы и интеллект разработчика средств защиты от несанкционированного доступа. Подробно данная ситуация исследуется математической наукой в теории игр – модели поведения двух противоборствующих сторон. При этом различают антагонистические и неантагонистические игры, а также игры, в которых одной из сторон является человек, а другой – природа или компьютер. В последнем случае взаимодействие человека с компьютером осуществляется по определенному игровому алгоритму с целью обучения, тренировки, имитации обстановки и с развлекательными целями.

Особый интерес в криминалистическом аспекте изучения личности преступника представляют специалисты-профессионалы в области средств компьютерной техники. Они обладают следующей социально-психологической характеристикой. Представители данной специальности обычно весьма любознательны и обладают незаурядными интеллектом и умственными способностями. При этом они не лишены некоторого своеобразного озорства и спортивного азарта. Наращиваемые меры по обеспечению безопасности компьютерных систем ими воспринимаются в психологическом плане как своеобразный вызов личности, поэтому они стремятся во что бы то ни стало найти эффективные способы до-

казательства своего превосходства. Как правило, это и приводит их к совершению преступления. Постепенно некоторые субъекты рассматриваемой категории не только приобретают необходимый опыт, но и находят интерес в этом виде деятельности. В конечном итоге происходит переориентация их целеполагания, которое из состояния «бескорыстной игры» переходит в свое новое качество – увлечение занятием подобной «игрой» лучше всего совмещать с получением некоторой материальной выгоды. Это может проявляться у преступников как в открытой форме – в различных ситуациях при их общении с окружающими (знакомыми, друзьями, родственниками, сослуживцами), так и в закрытой – в форме внутренних мыслей и переживаний без каких-либо внешних проявлений. Последнее обычно присуще людям замкнутым по характеру, малообщительным. Другие же могут продемонстрировать перед знакомыми или сослуживцами, родственниками и другими людьми свои умения найти незащищенные места в компьютерной системе, а иногда и то, как эти слабости можно использовать в личных целях. Таким образом происходит развитие и перерождение любителя-программиста в профессионального преступника.

Особенностями, указывающими на совершение компьютерного преступления лицами рассматриваемой категории, являются:

– отсутствие целеустремленной, продуманной подготовки к преступлению;

– оригинальность способа совершения преступления;

– использование в качестве орудий преступления бытовых технических средств и предметов;

– непринятие мер к сокрытию преступления;

– совершение озорных действий на месте происшествия.

Ко второй группе преступников относятся *лица, страдающие* новым видом психического заболевания – *информационными болезнями, или компьютерными фобиями*. Указанная категория заболеваний вызывается систематическим нарушением информационного режима человека: информационным голодом, информационными перегрузками, сбоями темпоритма, неплановыми переключениями с одного информационного процесса на другой, дефицитами времени на настройку, информационным шумом. Изучением этих вопросов в настоящее время занимается новая, сравнительно молодая отрасль медицины – информационная медицина. С позиции данной науки человек рассматривается как универсальная саморегулирующаяся информационная система с установленным балансом биологической информации. Нарушение последнего под воздействием внешних или внутренних дестабилизирующих факторов как врожденного, так и приобретенного в процессе жизни индивида ха-

рактера (т. е. инстинктов и рефлексов) приводит к различного рода информационным болезням, среди которых наиболее распространены информационные неврозы. Иными словами, человек нуждается в равной степени как в физической, так и в информационной энергии (духовной или эмоциональной, как ее называли ранее). Когда ее мало – наступает информационный голод, когда ее много – человек страдает от информационных перегрузок (различного рода стрессов и эмоциональных срывов), приводящих при стечении определенных обстоятельств к аффективному состоянию. Кроме того, человеку необходимо, чтобы информация поступала в определенном нормированном режиме, зависящем от индивидуальных особенностей и свойств личности. Информация должна быть также адаптирована к каждой конкретной личности. Сам человек при этом должен быть психологически готов к ее восприятию (априорная настройка), войти в процесс по ее обмену, обработке и фиксации (закреплению) (апостериорная настройка) и постоянно выдерживать темпоритм. Нарушение одной из этих компонент информационного процесса приводит к потерям информации субъектом (нарушение памяти человека), преждевременной физической и умственной усталости и в конечном итоге перерастает в информационную болезнь.

В настоящее время в связи с оснащением рабочих мест персональными компьютерами в целях повышения скорости протекания информационных процессов и эффективности использования рабочего времени многие служащие попадают в различные стрессовые ситуации, некоторые из которых заканчиваются формированием компьютерных фобий. По существу это есть не что иное, как профессиональное заболевание. Основные симптомы его проявления следующие: быстрая утомляемость, резкие скачкообразные изменения артериального давления при аудиовизуальном или физическом контакте со средствами компьютерной техники, повышенное потовыделение, глазные стрессы, головокружение и головные боли, дрожь в конечностях, затрудненность дыхания, обмороки и т. д. В основе компьютерной фобии лежит страх перед потерей контроля над своими действиями. Ситуация осложняется тем, что страдающие фобией обычно знают об иррациональности их страха, однако это делает боязнь еще более сильной по принципу резонанса.

Третью и последнюю группу составляют *профессиональные компьютерные преступники с ярко выраженными корыстными целями*, так называемые профи. В отличие от первой переходной группы «любителей» и второй специфической группы «больных», преступники третьей группы характеризуются многократностью совершения компьютерных преступлений с обязательным использованием действий, направленных на их

сокрытие, и обладают в связи с этим устойчивыми преступными навыками. Преступники этой группы обычно являются членами хорошо организованных, мобильных и технически оснащенных высококлассным оборудованием и специальной техникой (нередко оперативно-технического характера) преступных групп и сообществ. Лиц, входящих в их состав, в большинстве своем можно охарактеризовать как высококвалифицированных специалистов, имеющих высшее техническое, юридическое либо экономическое (финансовое) образование. Именно эта группа преступников и представляет основную угрозу для общества, является кадровым ядром компьютерной преступности как в качественном, так и в количественном плане. На долю именно этих преступников приходится максимальное число особо опасных посягательств, совершенных с использованием средств компьютерной техники.

В профессионально-классификационном плане круг компьютерных преступников чрезвычайно широк. Обычно это различные категории специалистов и руководителей: бухгалтеры, кассиры, контролеры, табельщики, нормировщики, операторы бензозаправочных станций, программисты, инженеры, финансисты, банковские служащие, адвокаты, менеджеры, юристы, коммерческие директора, управляющие, начальники смен, отделов и служб и т. д. Всех их можно разделить на две основные группы исходя из классифицирующего признака категории *доступа к средствам компьютерной техники*:

– внутренние пользователи;

– внешние пользователи, где пользователь (потребитель) – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Пользователи бывают двух видов: зарегистрированные (санкционированные) и незарегистрированные (несанкционированные).

Преступниками из числа внешних пользователей обычно бывают лица, хорошо осведомленные о деятельности потерпевшей стороны. Их круг настолько широк, что не поддается какой-либо систематизации и классификации: им может быть любой, даже случайный человек. Например, представитель организации, занимающейся сервисным обслуживанием, ремонтом, разработкой программных средств компьютерной техники на договорной основе, представители различных контролирующих и властных органов или организаций, клиенты и просто хакеры.

Деятельность правоохранительных органов по предупреждению, выявлению, пресечению, раскрытию и расследованию компьютерных преступлений носит сложный, многогранный характер и требует применения значительного объема специальных знаний и соответствующих научно-технических средств.

2. ОСОБЕННОСТИ ВОЗБУЖДЕНИЯ УГОЛОВНЫХ ДЕЛ О ПРЕСТУПЛЕНИЯХ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

В процессе расследования преступлений, совершенных с использованием высоких технологий, выделяют несколько типовых следственных ситуаций, в том числе на этапе возбуждения уголовного дела. Предлагается следующая их ***классификация***:

1) ситуации, обусловленные поводом к возбуждению уголовного дела:

– заявление о преступлении, поступившее от потерпевшего;

– непосредственное обнаружение признаков преступления органом дознания;

– проверка сообщения, поступившего из оперативного источника;

– проведение специальных оперативно-технических мероприятий;

– материалы проверок финансово-хозяйственной деятельности;

– задержание лица на месте преступления с поличным;

– непосредственное обнаружение признаков преступления следователем при расследовании другого преступления;

2) ситуации, складывающиеся к началу расследования:

– нет информации о причинах возникновения общественно опасных деяний, способе их совершения и личности правонарушителя;

– есть сведения о причинах преступления, способе его совершения, но нет сведений о личности преступника;

– известны причины преступления, способы его совершения и сокрытия, личность преступника и другие обстоятельства;

3) ситуации, обусловленные наличием сведений о владельце информации:

– собственник информационной системы известен;

– владелец информации не установлен;

4) ситуации, обусловленные наличием у собственника информационной системы сведений о нарушении целостности (конфиденциальности) информации в системе:

– собственник сам обнаружил противоправное деяние;

– о нарушении целостности (конфиденциальности) информации в системе собственнику неизвестно;

5) ситуации, обусловленные отношением собственника информационной системы к тому факту, что в отношении его было совершено противоправное деяние:

– собственник информационной системы знал, что в отношении его было совершено противоправное деяние, но не заявил об этом в правоохранительные органы;

– собственник информационной системы после обнаружения факта совершения противоправного деяния обратился в правоохранительные органы с заявлением о преступлении;

6) ситуации, обусловленные тем, известно ли лицо, совершившее противоправное деяние:

– лицо, совершившее противоправное деяние, известно;

– лицо, совершившее противоправное деяние, неизвестно.

На первоначальном этапе расследования могут быть также использованы *типовые следственные ситуации.* Это важно для своевременного выявления и последующего исследования следов преступления (в виде изменения компьютерной информации):

1) ситуации в зависимости от отношения собственника компьютерной информации к результатам поиска следов преступления:

– собственник компьютерной информации оказывает противодействие поиску компьютерной информации;

– собственник компьютерной информации активно содействует расследованию преступления;

– собственник компьютерной информации относится к расследованию безразлично;

2) ситуации, обусловленные наличием данных о защите информации в персональном компьютере при проведении следственного осмотра:

– имеются данные о наличии системы защиты в персональном компьютере, подлежащем осмотру;

– информация о наличии или отсутствии системы защиты отсутствует;

3) ситуации, обусловленные наличием сведений о количественных показателях осматриваемых предметов:

– на месте проведения следственного действия имеется сеть персональных компьютеров;

– на месте проведения следственного действия имеется один персональный компьютер.

Выделяют следственные ситуации в зависимости от энергетического состояния компьютера:

– компьютер подключен к общей энергетической сети;

– компьютер имеет автономную систему питания.

Исходя из сложившейся следственной ситуации по энергетическому состоянию компьютера или компьютерной системы, следователь должен предпринять меры по предотвращению возможного отключения энергетического питания в тех случаях, когда компьютеры подключены к общей энергетической сети.

Выделение следственных ситуаций в зависимости от функционального состояния компьютера нецелесообразно, так как состояние и внешние признаки предметов отражают в протоколе следственного действия.

В зависимости от *объема информации*, имеющейся у следствия, выделяют следующие *следственные ситуации*:

– отсутствует информация о способе, мотивах совершения преступления, личности злоумышленника, известны только последствия преступного деяния;

– известны способ, мотивы и последствия преступного деяния, но неизвестна личность злоумышленника;

– имеется информация о способе, мотивах и личности злоумышленника.

Указанная классификация определяется объемом информации, имеющейся у следователя на первоначальном этапе расследования. Первая следственная ситуация характеризуется наименьшим объемом информации, а последняя – наибольшим. Исходя из имеющихся данных, следователь определяет дальнейшее направление расследования и планирует проведение тех или иных следственных действий для получения недостающей информации.

Конкретные следственные ситуации определяют ***выбор оперативных и следственных действий, тактику их проведения***. Выделение следственных ситуаций на различных этапах расследования помогает следователю в выборе правильного направления расследования. Направления расследования определяются исходными данными, имеющимися в первоначальный период расследования, т. е. в период, когда еще неизвестно, какое именно преступление совершено, а действовать необходимо оперативно, по горячим следам.

Деятельность по выявлению, расследованию и предупреждению преступлений объективно невозможна без объединения усилий ряда правоохранительных и иных органов. Взаимодействие представляет форму использования специфических возможностей нескольких органов для достижения промежуточных и конечных целей их деятельности.

При расследовании преступлений в сфере высоких технологий могут реализовываться все виды ***взаимодействия следователя с соответствующими органами***. Однако взаимодействие с оперативными сотрудниками органов дознания является наиболее распространенным

и продуктивным. Сущность взаимодействия следователя и сотрудника оперативного подразделения выражается прежде всего в объединении их усилий при раскрытии преступлений, в согласованности действий при строжайшем соблюдении законности и самостоятельном выполнении каждым из них своих обязанностей при руководящей роли следователя.

Один из наиболее распространенных видов взаимодействия – *содействие органа дознания* при осуществлении следователем процессуальных действий. Тактические основания участия сотрудников оперативных подразделений в следственных действиях классифицируются на две группы.

Первая группа предусматривает активное участие в следственных действиях, связанных с получением, оценкой, проверкой оперативным сотрудником процессуально и криминалистически значимой информации (получение оперативным сотрудником процессуально и криминалистически значимой информации о расследуемом событии в оперативно-розыскных целях; оказание содействия следователю в реализации в ходе следственных действий информации, полученной оперативным путем; оказание следователю содействия в получении и проверке доказательственной информации по уголовному делу).

Вторая группа отражает необходимое *вспомогательное участие оперативного сотрудника*, выражающееся в обеспечении им нормального режима проведения следственных действий.

На практике взаимодействие в основном реализуется в рамках производства по конкретному уголовному делу, чаще всего с оперативными сотрудниками, осуществлявшими проверку данного материала до передачи его следователю. Единовременное, или разовое, взаимодействие имеет место и тогда, когда следователь дает поручение сотруднику конкретного подразделения (например, по раскрытию преступлений в сфере высоких технологий, по наркоконтролю и противодействию торговле людьми, по борьбе с экономической преступностью).

По результатам оперативно-розыскной деятельности полученная информация представляется следователю. Представление сведений о результатах проделанной работы предполагает анализ собранных материалов. Значение информационно-аналитической работы существенно возрастает при расследовании преступлений в сфере высоких технологий. Использование продуктов современных информационных технологий в решении различных аналитических задач позволяет существенно повысить качество и эффективность информационно-аналитической работы следователей и оперативных сотрудников при расследовании преступлений.

Такое взаимодействие позволяет объединенными силами с использованием возможностей обеих сторон осуществлять совместную деятель-

ность по выявлению, раскрытию преступлений, розыску виновных, а также пресечению замышляемых и подготавливаемых уголовно наказуемых деяний. Хорошо налаженное взаимодействие между следователем и органом дознания является важной предпосылкой эффективности и качества предварительного расследования.

Для преступлений, совершаемых в сфере высоких технологий, существенным фактором может являться межрегиональный, а иногда и межгосударственный характер совершаемых деяний. В связи с развитием компьютерной техники образовался целый ряд новых областей сотрудничества государств, в том числе по вопросам правовой охраны программного обеспечения и баз данных, информации при ее использовании в компьютерных сетях, а также содействия процессу информатизации, обмена компьютерными технологиями. Наиболее важные из них – области сотрудничества, связанные с предупреждением и пресечением правонарушений, препятствующих правомерному использованию компьютеров и компьютерных сетей. Между тем наибольшей общественной опасностью обладают преступления, при совершении которых компьютерная техника выступает объектом либо средством преступного посягательства. В этом случае возникает необходимость во взаимодействии органов следствия и дознания как между собой, так и с иными государственными и негосударственными структурами.

Важным организационно-правовым вопросом, связанным со спецификой расследования преступлений в сфере высоких технологий, является проблема *взаимодействия следствия, органа дознания с аналогичными органами других государств*.

При осуществлении взаимодействия в различных сферах системы правоохранительных органов используются две основные правовые формы: договорно-правовая форма – заключение и реализация договоров по международному сотрудничеству разных стран в сфере расследования преступлений; институционная форма – сотрудничество в рамках международных организаций различного уровня, например ООН, Интерпол, Совет Европы (Глобальная программа действий по борьбе с киберпреступностью (GLACY)) и др.

Правовой базой для такого взаимодействия в странах СНГ является Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (1993), к которой присоединились Республика Армения, Республика Беларусь, Республика Казахстан, Кыргызская Республика, Республика Молдова, Российская Федерация, Республика Таджикистан, Туркменистан, Республика Узбекистан, Украина. Типовым соглашением, которое является приложением к данному

постановлению, предусмотрено, что его стороны будут осуществлять взаимодействие в предупреждении, выявлении, пресечении и раскрытии преступлений в различных сферах. Однако преступные действия в области компьютерной информации в документе отражения не нашли, что является его недостатком. В 2001 г. на уровне СНГ в Минске было подписано Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации. В 2009 г. в рамках Соглашения правительств государств – участников СНГ об обмене информацией в сфере борьбы с преступностью также предусмотрена возможность представления информации о подозреваемых, обвиняемых в совершении преступлений и осужденных за совершение преступлений в сфере высоких технологий.

В настоящее время большинство государств признают угрозу киберпреступности в качестве мировой проблемы. В связи с этим принимаются акты международно-правового характера, свидетельствующие о взаимодействии государств, и соглашения между отдельными государствами о взаимопомощи. По делам об информационных преступлениях при наличии такого соглашения следствие располагает возможностями как осуществить необходимые процессуальные действия, так и скоординировать проведение оперативно-розыскных мероприятий. Для тех стран, с которыми подобные правовые соглашения не заключены, возможности координации усилий по расследованию весьма ограничены.

Важным шагом, направленным на противодействие киберпреступности, стало принятие в 2001 г. Советом Европы Конвенции о преступности в сфере компьютерной информации, вступившей в силу с 1 января 2004 г. Этот документ стал одним из первых международных соглашений по юридическим и процедурным аспектам взаимодействия при расследовании киберпреступлений. Конвенцией предусмотрены скоординированные действия на национальном и межгосударственном уровнях по пресечению несанкционированного вмешательства в работу компьютерных систем, незаконного перехвата данных. Однако без реальных механизмов реализации положений Конвенции на национальном уровне этот документ носит только декларативный характер. Республика Беларусь не присоединилась к данной Конвенции, что является негативным моментом и препятствует формированию единой системы взаимодействия правоохранительных органов при расследовании преступлений в сфере высоких технологий.

Существенную помощь в процессе расследования преступлений, особенно транснациональных и трансграничных, совершенных в сфере высоких технологий, может оказать *Интерпол*, имеющий свои национальные

бюро практически во всех странах. Возможности Интерпола используются в процессе розыска и идентификации лиц, выявления, предупреждения, пресечения и раскрытия преступлений, имеющих международный характер. По каналам Интерпола исполняют запросы, поступающие от правоохранительных органов иностранных государств и международных правоохранительных организаций. Информационное обеспечение сотрудничества взаимодействующих органов с правоохранительными органами иностранных государств – членов Интерпола и генеральным секретариатом осуществляют национальные центральные бюро Интерпола.

Кроме того, в Республике Беларусь была внедрена система национальных корреспондентских пунктов I-24/7 (двадцать четыре часа в день семь дней в неделю), создание которой было предусмотрено Конвенцией о преступности в сфере компьютерной информации 2001 г.[1] По каналам телекоммуникационной сети Интерпола I-24/7 осуществляется информационный обмен с генеральным секретариатом и национальными центральными бюро Интерпола иностранных государств для обмена документами, изображениями фотографий и дактилоскопических карт, конфиденциальными документами, а также для обмена информацией со специализированным банком данных генерального секретариата.

Появление этой системы обусловлено потребностями практики. При расследовании киберпреступлений для установления преступника необходимо проследить весь «путь» совершения преступления. Это значит, что следователь должен обладать информацией о всех серверах, которые использовал преступник для совершения преступления. Как правило, их десятки, а иногда и сотни. С введением системы национальных корреспондентских пунктов в этой области произошло много изменений. Теперь информация на сервере хранится значительно дольше. Запросы отправляют в электронном виде через сеть центров системы национальных корреспондентских пунктов и через них же получают ответы, что существенно облегчает не только сбор доказательств, но и установление места нахождения виновных лиц. По соответствующим запросам о преступлениях, совершенных в сфере высоких технологий, может быть получена информация:

– о сетевых адресах, именах доменов и серверов организаций и пользователей; о содержании протоколов, логических файлов;

– электронной информации, заблокированной в порядке оперативного взаимодействия правоохранительных органов при пресечении трансграничных правонарушений; о провайдерах и дистрибьюторах сетевых и телекоммуникационных услуг;

[1] Подробнее см.: I-24/7 [Электронный ресурс]. URL: https://www.interpol.int/INTERPOL-expertise/Data-exchange/I-24-7.

– физических и юридических лицах, имеющих отношение к преступлениям в сфере высоких технологий;

– специализированном программном обеспечении, методиках и тактике борьбы с компьютерными и телекоммуникационными преступлениями, периодических и специальных изданиях, обзорах статистики, материалах о деятельности специализированных служб различных государств в данной области.

В запросах о преступлениях, совершенных в области высоких технологий, направляемых в национальные центральные бюро Интерпола, должны быть указаны следующие сведения:

– основания проведения проверки;

– вид преступления, место и время его совершения (если известно);

– лица, причастные к преступлению;

– потерпевший (физическое или юридическое лицо), характер и размер нанесенного ущерба;

– способ совершения преступления, в том числе технические средства, программное обеспечение, используемое в преступных целях, а также время и продолжительность неправомерного доступа;

– иная информация, которая может облегчить исполнение запроса.

Запросы подготавливаются на русском языке, но наименования сетевых адресов, имен доменов и серверов организаций и пользователей должны быть указаны на языке оригиналов. Этот пункт является очень важным, так как наименования сетевых адресов, доменов и серверов организаций, а иногда и имена пользователей пишутся в оригинале на английском языке. Неправильное их написание может привести к ошибкам при проведении следственных действий и оперативно-розыскных мероприятий и, соответственно, к увеличению времени расследования.

Одна из проблем использования результатов оперативно-розыскной деятельности в процессе расследования преступлений – можно ли опираться на эти результаты при принятии решений о производстве процессуальных действий? Р.С. Белкин полагал, что результаты оперативно-розыскных действий могут служить основанием только для проведения следственных действий, направленных на закрепление и обнаружение доказательств (осмотр, обыск, выемка). Критерием использования таких данных должно быть также обеспечение при производстве следственных действий законных прав и интересов граждан.

В последние годы в связи с распространением сети Интернет и постоянным увеличением числа ее пользователей актуальным стало размещение в сети ориентирующей информации о разыскиваемых лицах. Наиболее перспективными направлениями *использования интернет-ре-*

сурсов для нужд розыска являются размещение информации на официальных сайтах МВД, ГУВД, УВД, использование баннеров (всплывающих картинок) на различных сайтах, отсылка сообщений по электронным адресам различных государственных организаций.

Наиболее общие рекомендации по обращению через средства массовой информации: обращение не должно носить сенсационный характер; формулировка обращения должна содержать минимум исходных данных, необходимых для ответа на вопросы, поставленные органом дознания; нельзя разглашать сведения о частной жизни лица. Описание разыскной информации о лицах в сети Интернет имеет ряд особенностей: наличие ярких красок в общем оформлении разыскной информации; использование подчеркивания, жирного шрифта, красной строки, абзаца; наличие фотографии или цветного фоторобота; указание на причины, по которым то или иное лицо разыскивается; описание противоправного деяния, в совершении которого разыскиваемое лицо подозревается; использование метода радиантного мышления (ассоциативных мыслительных процессов, отправной точкой которых является центральный объект) при изложении разыскного описания.

Практика свидетельствует, что процесс раскрытия преступной деятельности организованных преступных групп и сообществ чаще всего начинается с оперативно-розыскной негласной деятельности, в ходе которой выявляется существование той или иной преступной организации и собираются данные о ее криминальной деятельности.

Такое соотношение и взаимообусловленность процессуальной деятельности по расследованию преступлений в сфере высоких технологий и оперативно-розыскной деятельности обусловливают соответствующее соотношение между доказательствами и непроцессуальной информацией, полученной до возбуждения уголовного дела.

Следователю представляются результаты оперативно-розыскной деятельности, которые соответствуют установленным ведомственными нормативными актами требованиям и могут:

– служить поводом и основанием для возбуждения уголовного дела;

– быть использованы для подготовки и осуществления следственных и судебных действий;

– использоваться в доказывании по уголовным делам в соответствии с требованиями уголовно-процессуального законодательства, регламентирующими собирание, проверку и оценку доказательств.

Органы, осуществляющие оперативно-розыскную деятельность и представившие ее результаты в уголовный процесс, обязаны представить следователю данные, необходимые для формирования, проверки и

оценки доказательств, полученных на основе результатов оперативно-розыскной деятельности.

Задача следователя – четко определить цели и направление оперативной работы. Для того чтобы это сделать, а затем иметь возможность проверить результаты проделанной работы, следователь должен прежде всего представлять себе возможные пути раскрытия преступления. Для этого необходимо оперировать несколькими версиями, что обусловит четкую постановку задач при направлении поручений органу дознания.

Источник информации, материальный носитель, след возникают на непроцессуальной стадии ее формирования, когда событие преступления оставляет изменения в сознании людей или следы на материальных объектах. Взаимодействие предметов объективного мира влечет за собой их взаимную трансформацию и создает возможности передачи соответствующей информации. Однако следы сами по себе еще не являются доказательствами.

Следует отметить вопрос о признании в качестве источника доказательств различных электронных документов. В соответствии с ч. 2 ст. 88 Уголовно-процессуального кодекса Республики Беларусь (далее – УПК) к числу ***источников доказательств*** относятся иные документы и другие носители информации, полученные в порядке, предусмотренном УПК. Согласно ст. 100 УПК такие документы и носители информации признаются источниками доказательств, если обстоятельства и факты, изложенные в них, удостоверены должностными лицами организаций или гражданами и имеют значение для уголовного дела. К другим носителям информации относятся материалы фото- и киносъемки, звуко- и видеозаписи и иные носители информации, полученные, истребованные или представленные в порядке, предусмотренном ст. 103 УПК. В соответствии с данным определением в качестве источника доказательств рассматриваются не сами электронные документы, а *протоколы* соответствующих *следственных действий*, в ходе которых такие документы исследовались, например протоколы осмотров. Целесообразно подробно описывать в указанных протоколах электронные документы по правилам описания традиционных письменных документов с точным указанием их месторасположения (пути) на носителе информации и свойств содержащего документ файла. При этом при наличии возможности электронный документ должен быть распечатан и приобщен в качестве приложения к протоколу осмотра. Носитель информации с электронным документом, содержащим признаки вещественного доказательства, подлежит приобщению в качестве такового к материалам уголовного дела. Также целесообразно независимо от возможности фак-

тического приобщения к делу первоначального носителя с электронным документом изготавливать в ходе осмотра копию представляющего интерес для следствия электронного документа на отдельном носителе (диске и др.) и приобщать такой носитель с электронным документом в опечатанном виде в качестве приложения к протоколу осмотра.

Помимо изложенного электронный документ может найти свое отражение и в таком источнике доказательств, как *заключение эксперта* по результатам проведения по делу компьютерно-технической экспертизы. Согласно положениям ст. 89 УПК при производстве по уголовному делу подлежат доказыванию:

1) наличие общественно опасного деяния, предусмотренного уголовным законом (время, место, способ и другие обстоятельства его совершения);

2) виновность обвиняемого в совершении преступления;

3) обстоятельства, влияющие на степень и характер ответственности обвиняемого (обстоятельства, смягчающие и отягчающие ответственность, характеризующие личность обвиняемого);

4) характер и размер вреда, причиненного преступлением.

По уголовным делам о совершении преступлений несовершеннолетними подлежат установлению и дополнительные обстоятельства, указанные в ч. 2 названной статьи УПК.

Согласно сложившейся практике *доследственная проверка по заявлениям и сообщениям* о совершении преступлений расследуемой категории осуществляется органами дознания, преимущественно территориальными отделами управления по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь, исходя из чего работники предварительного расследования вступают в процесс доказывания на стадии ***возбуждения уголовного дела*** после поступления материалов проверки. В соответствии с требованиями ст. 27 УПК орган уголовного преследования в пределах своей компетенции обязан возбудить уголовное дело в каждом случае обнаружения признаков преступления. При этом не требуется, чтобы в ходе проверки были исчерпывающим образом установлены все обстоятельства, входящие в предмет доказывания по делу, достаточно фиксации основных признаков состава соответствующего преступления. Так, для возбуждения уголовного дела достаточно наличия в материалах проверки доказательств, подтверждающих событие преступления, общих сведений относительно его механизма и общественно опасных последствий. При установлении лица, предположительно совершившего исследуемое общественно опасное деяние, в материалах проверки должны содержаться сведения относи-

тельно его соответствия требованиям к субъекту данного преступления. Неустановление в ходе проверочных мероприятий правонарушителя не может являться основанием к возвращению материалов для производства дополнительной проверки либо к отказу в возбуждении уголовного дела. При принятии решения о возбуждении уголовного дела исходя из оценки собранных в ходе проверки доказательств осуществляется планирование дальнейшего расследования в целях *проверки имеющихся доказательств и собирания дополнительных* для обеспечения полноты, всесторонности и объективности предварительного расследования.

В дальнейшем эти факты воспринимаются и процессуально закрепляются лицами, осуществляющими расследование. Органы, уполномоченные законом, с соблюдением установленных требований выявляют и собирают их, придавая им форму протоколов, показаний, признавая вещественными доказательствами, документами и прочими видами доказательств, установленными УПК. До тех пор, пока не возникло производство по уголовному делу и не началось применение норм, регулирующих собирание доказательств, нельзя говорить о наличии процессуальной формы доказательств. При этом информация становится доказательственной, закрепленной в определенной процессуальной форме, момент начала ее существования в качестве таковой связан с моментом процессуального закрепления. Уголовно-процессуальное законодательство предусматривает правила собирания, проверки и оценки различной информации и придания ей доказательственного значения.

Таким образом, для того, чтобы система доказательств была убедительной, необходимо, чтобы деятельность по ее формированию обеспечивалась *оперативно-розыскной деятельностью*. И это особенно важно при формировании системы доказательств по делам о преступлениях в сфере компьютерной информации. Причиной здесь является то, что наличие связи между отдельными доказательствами часто необходимо устанавливать и проверять с помощью информации, которую получают в ходе проведения оперативно-розыскных мероприятий. Причем сама информация, полученная в результате проведения оперативно-розыскных мероприятий, является не более чем средством, применяя которое, правоохранительные органы пытаются воссоздать картину совершенного преступления. С ее помощью выявляются источники достоверной информации, которая может стать доказательственной. Кроме того, компьютерные технологии в целом отличаются тем, что они достаточно сложны в понимании, а потому лица, виновные в совершении преступлений с их использованием, имеют возможность запутать и следствие, и суд. В связи с этим вполне очевидна сложность и в понимании от-

дельных доказательств, из которых следователю необходимо сформировать систему, уличающую в совершении преступления конкретных лиц. Отдельные, вне какой-либо системы доказательства выглядят достаточно многозначно, а потому не имеют убедительности, необходимой для изобличения виновных лиц. Именно это характерно для доказательств, которые собираются при расследовании преступлений в сфере высоких технологий. Для того чтобы преодолеть названную многозначность, понять то, в какой связи доказательства находятся друг с другом, необходима информация, которая бы подтверждала и указывала на наличие этих связей. С этой целью необходимо, чтобы одновременно с системой доказательств формировалась и система оперативно-розыскной и иной информации. Система информации, полученной благодаря оперативно-розыскным мероприятиям, помогает выявить связи между доказательствами, что способствует формированию системы доказательств.

Также значение оперативно-розыскного сопровождения расследования преступлений в сфере компьютерной информации состоит в том, чтобы упредить действия лиц, не заинтересованных в установлении истины по делу, направленные на дискредитацию собранных следователем и лицами, оказывающими ему содействие, доказательств. В этой части значение оперативно-розыскной информации состоит в том, что, располагая ею, можно укрепить имеющиеся доказательства, например, проведением соответствующей экспертизы или иными следственными действиями. В итоге может быть создана система доказательств, убедительно подтверждающая выводы следователя, к которым он пришел в результате проведенного расследования.

3. ТАКТИКА ПРОВЕДЕНИЯ ОСМОТРОВ, ОБЫСКОВ И ВЫЕМОК ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

В последние годы в Республике Беларусь сохраняется общая тенденция роста преступлений в сфере высоких технологий, что объясняется объективными причинами. Изучение международного опыта показывает, что такая тенденция свойственна большинству государств мира. Количество преступлений в указанной сфере увеличивается и будет увеличиваться в ближайшем будущем в связи с бурным развитием информационных и телекоммуникационных технологий, стремительным увеличением количества электронных устройств и услуг, предоставляемых населению с использованием информационных технологий.

Развитие информационных технологий, в том числе и в Беларуси, привело к видоизменению старых и появлению новых форм противоправной деятельности, связанных с использованием различных компьютерных систем.

Преступления против информационной безопасности приобретают транснациональный, организованный и групповой характер. С использованием телекоммуникационных сетей и компьютеров преступление может быть совершено на территории другой страны и даже нескольких государств одновременно, при этом преступник потратит на его совершение всего несколько минут и будет общаться с представителями различных организаций (банковские учреждения, интернет-магазины, платежные системы), не выходя из своего дома.

В настоящее время для совершения и сокрытия подобного рода преступлений используются как персональные компьютеры, так и мобильные телефоны, различные платежные инструменты, задействуются возможности, предоставляемые ресурсами сети Интернет.

Персональный компьютер, еще относительно недавно являвшийся достоянием довольно узкого круга специалистов и избранных лиц, в настоя-

щее время общедоступен и необходим как для работы, так и для использования в повседневной жизни большинством населения нашей страны.

Одним из важнейших доказательств по уголовным делам о преступлениях в сфере высоких технологий являются данные, содержащиеся на машинных носителях информации компьютеров.

Своевременное получение таких доказательств и их дальнейшая проверка позволят использовать «электронные следы» для установления обстоятельств, имеющих значение для правильного разрешения уголовного дела. В связи с этим следователи должны знать, каким образом они могут обнаружить, зафиксировать и изъять подобные доказательства.

Осмотр места происшествия, помещений, обыск и выемка по уголовным делам о преступлениях в сфере высоких технологий являются важнейшими следственными действиями, от результатов которых во многом зависит характер проводимого впоследствии расследования.

Так, при успешной организации и проведении указанных следственных действий могут быть обнаружены и изъяты различные средства компьютерной техники, содержащие порой бесценную информацию, необходимую для расследования уголовного дела.

Указанные следственные действия требуют тщательной подготовки.

На ***подготовительном этапе*** необходимо осуществить следующие мероприятия:

– установить, какие средства компьютерной техники могут находиться в месте проведения следственного действия, а также порядок доступа к ним (при проведении действий в помещении какой-либо организации) и информации, содержащейся на машинных носителях информации;

– изучить личность подозреваемого либо иного лица, у которого будут проводиться следственные действия, в том числе его профессиональные навыки пользования компьютером, а также средствами шифрования;

– определить круг лиц, которые будут участвовать в следственном действии, в том числе специалистов в области информационной безопасности, проинструктировать их о порядке проведения действий, а также характере предметов и информации, которые подлежат обнаружению и изъятию;

– подготовить необходимые технические и программные средства, позволяющие осуществлять просмотр, поиск, изъятие и последующее хранение компьютерной информации;

– определить дату, время и место следственного действия, а также предпринять меры по обеспечению конфиденциальности действий.

Перед началом следственного действия следователь должен четко представлять, что надо искать и где, а также принять решение о способе изъятия компьютерной информации, так как от этого будет зависеть тактика следственного действия.

По ***прибытии к месту проведения следственного действия*** необходимо выполнить следующие мероприятия:

– по возможности максимально быстро войти в помещение, подлежащее осмотру;

– при оказании сопротивления со стороны лиц, находящихся в помещении, принять действенные меры по нейтрализации противодействия и скорейшему проникновению в помещение;

– организовать охрану места следственного действия и наблюдение за ним в целях противодействия возможному уничтожению информации, а также попыткам экстренного выключения средств компьютерной техники, в том числе путем обесточивания электропитания, применения специальных средств защиты (шифрования, уничтожения информации).

В связи с этим все электротехнические приборы, расположенные на месте проведения следственного действия, должны находиться до момента их осмотра в том положении и техническом состоянии, в котором они были в момент начала следственного действия. Для этого необходимо:

– не разрешать каким-либо лицам прикасаться к средствам компьютерной техники и иным техническим средствам, а также источникам питания электрооборудования с любой целью, даже в случае согласия лица, у которого проводится следственное действие, добровольно выдать требуемый предмет или информацию;

– не разрешать каким-либо лицам без разрешения специалиста выключать или включать электроснабжение.

На *обзорной стадии следственного действия* необходимо установить:

– количество и места расположения средств компьютерной техники и их типы;

– наличие локальной сети и места расположения серверов (на которых могут храниться различные образы памяти) и выхода в другие сети с помощью модема или выделенных линий;

– используемое системное и прикладное программное обеспечение;

– наличие систем защиты информации, их типы;

– возможность использования средств экстренного уничтожения компьютерной информации.

При наличии компьютерной сети любого уровня технической организации в первую очередь должен быть осмотрен сервер сети, который хранит в своей оперативной и постоянной памяти наибольшую часть компьютерной информации, управляет другими компьютерами, имеет с ними прямую связь и, как правило, программу автоматической фиксации

доступа друг к другу (своеобразный «электронный журнал» учета работы всех компьютеров сети, точные даты и время каждого соединения при обмене информацией, длительность и вид сеанса связи, характеристику передаваемой и получаемой информации, аварийные ситуации, сбои в работе отдельных рабочих станций, периферийного оборудования, идентификационные имена и пароли операторов).

Следователь должен знать, что при наличии соединения средств компьютерной техники с другим оборудованием, находящимся вне периметра зоны проводимого следственного действия (в другом помещении, здании, населенном пункте и т. д.), существует реальная возможность непосредственного доступа к компьютерной информации и совершения любых действий с ней (уничтожение, модификация, копирование либо блокирование). Для предотвращения этого необходимо временно или на длительный срок отключить компьютерную технику или локальную вычислительную сеть целиком от технических устройств, находящихся за периметром зоны осмотра. Отключение может быть произведено как на программном, так и аппаратном уровне.

Если специалисту удастся установить, что в ходе следственного действия на каком-либо устройстве происходит уничтожение информации либо уничтожается машинный носитель информации, необходимо всеми возможными способами приостановить этот процесс и начать обследование с данного места.

В *ходе следственного действия* также необходимо определить компьютеры, находящиеся во включенном состоянии, и характер выполняемых ими процессов и программ. Так, необходимо:

– с участием специалиста установить перечень выполняемых программ и процессов, а также определить наличие информации, к потере которой может привести некорректное выключение компьютера;

– определить и отключить специальные средства защиты информации от несанкционированного доступа, принять меры к установлению пароля для шифрования-дешифрования информации либо к получению защищенной информации.

Так, если на исследуемом компьютере используются программы, предназначенные для шифрования информации, либо содержится информация, доступ к которой требует авторизации, при этом доступ к указанной информации открыт, то необходимо скопировать такую информацию на внешний машинный носитель информации. При этом в протоколе следственного действия следует детально указать все программы и производимые действия (желательно осуществление моментальных снимков экрана (так называемые скриншоты), фотосъемки либо видеозаписи).

Если же компьютер будет выключен без выяснения и фиксации указанных обстоятельств, то доступ к защищенной информации будет закрыт, а отсутствие у следователя необходимых реквизитов (например, имени пользователя и (или) пароля) не позволит использовать указанную информацию в качестве доказательства.

Для получения всей возможной доказательственной информации следователь должен знать перечень компьютерной техники, которая обладает свойствами хранения информации и в данной связи имеет наибольший интерес для расследования уголовного дела, поскольку способна предоставить основные доказательства преступной деятельности преступника.

Свойствами хранения компьютерной информации обладают следующие средства компьютерной техники: устройство HDD (Hard Disk Drive, накопитель на жестких магнитных дисках, жесткий диск, винчестер), устройство внешний HDD, устройство Flash USB Drive (флэш-накопитель, флэшка), устройство Flash-memory (флэш-память, карта памяти, флэшка), оптический (лазерный) диск, планшетный компьютер (электронный планшет), мобильный телефон или смартфон; электронная книга (цифровая книга), цифровые фото- и видеокамеры; MP3-плеер; игровая приставка, GPS-навигатор. Данный перечень в связи с постоянным развитием сферы высоких технологий не является исчерпывающим и должен пополняться.

Одним из наиболее важных следственных действий при осмотре места происшествия по делам рассматриваемой категории является ***изъятие средств компьютерной техники***.

Существуют два основных *способа изъятия компьютерной информации*:

– изъятие обнаруженных средств компьютерной техники с последующим детальным изучением имеющейся на них компьютерной информации вне места изъятия (например, в служебном кабинете или в экспертном учреждении);

– изучение всех средств компьютерной техники (содержащейся на них компьютерной информации) непосредственно во время следственного действия с последующим изъятием только той ее (компьютерной информации) части, которая представляет интерес для дела.

Каждый способ имеет свои преимущества. Изъятие всех средств компьютерной техники ускоряет сам процесс осмотра (обыска, выемки), дает возможность направить все силы на поиск иных материальных следов, имеющих отношение к расследованию преступления, снижает психологическую нагрузку на граждан, не требует привлечения высококвалифицированного специалиста в области информационных техно-

логий к непосредственному участию в следственном действии, так как методикой изъятия средств компьютерной техники должен обладать и сам следователь.

К несомненным достоинствам такого подхода можно отнести и возможность в последующем более детально изучить всю информацию, имеющуюся на компьютерах, с привлечением специалистов. Это практически исключает возможность необнаружения даже профессионально сокрытой информации.

Следовательно, по возможности необходимо всегда изымать машинный носитель информации для дальнейшего его детального осмотра. При этом достаточно ограничиться описанием в протоколе следственного действия внешних отличительных признаков носителя (тип, модель, серийный номер, имеющиеся надписи). Изымать целиком системный блок компьютера и тем более периферийное оборудование не имеет смысла, поскольку они, как правило, не содержат интересующей следствие компьютерной информации.

В конкретной следственной ситуации (уголовные дела по факту использования реквизитов доступа в сеть Интернет, несанкционированного доступа к различным ресурсам и т. д.) возможно изъятие системного блока компьютера или модема, которые содержат сведения о MAC-адресе (MAC – Media Access Control – адрес единицы оборудования в сети).

Однако иногда существуют технические и психологические сложности изъятия всех средств компьютерной техники (объединение компьютеров в разнообразные сети, возможность потери информации при отключении и т. д.) или такое изъятие нецелесообразно.

Если изъять сам носитель информации не представляется возможным, но возможно выключение компьютера на некоторое время, то необходимо при проведении следственных действий создание точной копии носителя (так называемого образа памяти или побитовой копии, которые создаются специальными программами, например EnCase или Acronis True Image), с которой впоследствии возможно работать так же, как с оригинальным носителем.

Следует помнить, что выход из строя компьютерных систем банков и ряда организаций (отсутствие в них отдельных компьютеров) может привести к полной дезорганизации их работы и значительным материальным убыткам, что грозит претензиями пострадавших организаций. Вследствие этого иногда рекомендуется применять второй способ: изъятие информации из средств компьютерной техники непосредственно в ходе следственного действия. В таких случаях в целях снижения вероятности необнаружения сокрытой информации или ошибок непосредственно при изъятии информации в обязательном порядке необходимо привлекать специалистов в компьютерной технике и (или) информатике (программиста, системного администратора, специалиста по сетевому оборудованию и др.).

Особенность данной ситуации – ограниченность во времени, поэтому исключительно важно привлечь именно высококвалифицированного специалиста и правильно его сориентировать относительно искомой информации, которая может иметь значение для дела.

Второй важный момент – наличие необходимых для изъятия информации технических средств, например портативного компьютера, внешних носителей информации и т. д. В любом случае каждая следственная ситуация уникальна, в связи с этим на выбор необходимого и подходящего способа изъятия машинных носителей информации средств компьютерной техники могут влиять различные обстоятельства. Конечное решение должен принимать следователь, исходя из складывающейся обстановки.

В протоколе следственного действия должно быть указано, в каком месте и при каких обстоятельствах были обнаружены изымаемые предметы, выданы они добровольно или изъяты принудительно. Все изымаемые предметы должны быть перечислены в протоколе с точным указанием количества, индивидуальных признаков, в том числе с описанием повреждений. В отношении средств компьютерной техники в протоколе также должно быть указано (при наличии соответствующей информации): полное заводское название, серийный номер устройства, дата производства, нахождение устройства во включенном или выключенном состоянии. Если машинный носитель информации изымается без устройства, в котором он находился, например извлеченный из системного блока накопитель на жестких магнитных дисках, то это также должно быть отражено в протоколе с описанием как изымаемого машинного носителя информации, так и устройства, из которого он был извлечен и которое непосредственно не изымается.

Если при проведении осмотра, обыска, выемки были предприняты попытки уничтожить или спрятать подлежащие изъятию предметы, выключить компьютерные устройства, удалить компьютерную информацию с машинных носителей информации, это должно быть отражено в протоколе следственного действия с указанием принятых мер.

Следует помнить, что порядок проведения следственных действий по изъятию средств компьютерной техники, как и любых иных вещественных доказательств, порядок процессуального оформления их поиска, изъятия и упаковки регулируется соответствующими нормами УПК, в частности ст. 204, 210, 212. При проведении перечисленных следствен-

ных действий приведенные нормы УПК должны неукоснительно соблюдаться. При их нарушении полученные доказательства могут быть признаны недопустимыми на стадии предварительного расследования или судебного разбирательства. Изъятие указанных средств, машинных носителей информации должно происходить при непосредственном участии соответствующих специалистов.

Следователь должен обеспечить строгое соблюдение требований уголовно-процессуального законодательства, иначе изъятые при производстве следственного действия средства компьютерной техники, материалы и документы впоследствии не смогут выступать в качестве доказательств по делу. Для успешного осуществления вышеуказанного требования необходимо придерживаться следующих рекомендаций:

1) по ходу проведения следственного действия необходимо постоянно акцентировать внимание понятых на всех производимых специалистами манипуляциях и их результатах;

2) фактическое изъятие средств компьютерной техники, находящихся на момент их осмотра во включенном состоянии, производится только после того, как будут выполнены и отражены в протоколе следующие действия:

– определено и корректно приостановлено выполнение вычислительной операции;

– информация, находящаяся в оперативной памяти средств компьютерной техники, записана на его постоянный машинный носитель информации либо на специально подготовленный и тестированный для этих целей внешний машинный носитель информации;

– определены и корректно закрыты все выполняемые программы (в некоторых случаях некорректное отключение средства компьютерной техники путем его перезагрузки или выключения электропитания без предварительного выхода из выполняемой программы приводит к потере информации, нарушению конфигурации вычислительной системы, стиранию всех информационных ресурсов на данном средстве компьютерной техники);

– выключено электропитание средства компьютерной техники и всех его периферийных устройств;

– все электропитающие и соединительные провода и кабели, имеющие разъемное соединение, отсоединены от средства компьютерной техники, источника питания и периферийного оборудования с обязательным указанием в протоколе порядка их соединения (принципиальной схемы), отсоединения и индивидуальных признаков каждого элемента.

Изымаемые средства компьютерной техники и их составляющие следует опечатывать так, чтобы исключить возможность непроцессуальной

работы с ними, разукомплектования и физического повреждения. Для достижения данной цели необходимо:

– в случае отсутствия у средства компьютерной техники электропитающего и соединительного (портового) разъемов наложить лист бумаги или бумажный конверт (колпак) на штепсельную и (или) соединительную вилку, зафиксировать его бечевкой на корпусе провода у основания вилки;

– лист (полоску) бумаги-пломбы следует также наложить на все разъемные детали корпуса средства компьютерной техники и его составляющих, скрепив их между собой, и зафиксировать (на прорезь дисковода, щель приемного устройства, лицевую и боковую панель, тыльную панель и корпус и т. д.);

– при наличии картонных коробок, ящиков, бумажных канцелярских или почтовых мешков и больших конвертов изымаемые средства компьютерной техники можно запаковать в них без соблюдения требований, указанных выше, но обязательно опломбировать все соединительные швы и сделать опись вложения;

– на листах пломбирующей бумаги, пломбах или упаковке должны быть подписи следователя, понятых и специалиста, участвующего в изъятии;

– машинные носители информации, документы, технические устройства, соединительные (электропитающие) провода и кабели вместе с разъемными устройствами надо упаковать отдельно друг от друга, сделать точное описание в протоколе каждого индивидуального признака и опись вложения для каждой единицы тары;

– при отсутствии четких внешних признаков изымаемый предмет следует запечатать в отдельную коробку (ящик, конверт), обязательно сделать об этом отметку в протоколе проведения следственного действия.

При изъятии магнитного носителя информации нужно помнить, что он должен перемещаться в пространстве и храниться исключительно в специальном экранированном контейнере или алюминиевом футляре (оболочке), исключающих разрушающее воздействие различных электромагнитных и магнитных полей и направленных излучений. Для этого магнитные носители информации сначала упаковывают в пакет из обычной фольги (бытового или технического назначения), а затем опечатывают обычным способом, вкладывая в коробку или конверт. В качестве контейнера можно использовать специальные экранированные контейнеры либо алюминиевую коробку с крышкой.

Если в коробку упаковывается несколько машинных носителей информации, то составляется опись вложения с указанием индивидуальных признаков каждого носителя. Недопустимо приклеивать что-либо

непосредственно к машинному носителю информации, пропускать через него бечевку, пробивать степлером, делать пометки или маркировки, накалывать твердым предметом знаки, использовать пластилиновые или сургучные печати и т. д.

В случае невозможности изъятия и приобщения к делу в качестве вещественного доказательства средства компьютерной техники (например, если оно является элементом компьютерной сети или системы дистанционной обработки информации) необходимо либо заменить изымаемое средство компьютерной техники дублирующим, аналогичным по характеристикам, либо изъять, если возможно, только машинный носитель информации, либо создать образ памяти машинных носителей информации изымаемого средства компьютерной техники.

Если возникла необходимость изъятия информации из оперативной памяти средства компьютерной техники (непосредственно из оперативного запоминающего устройства или его виртуального диска), то сделать это можно только путем копирования соответствующей информации на машинный носитель информации с использованием стандартных, специально подготовленных и тестированных программных и аппаратных средств компьютерной техники, тактико-технические характеристики и индивидуальные признаки которых обязательно должны быть отражены в протоколе проведения следственного действия. Процесс изъятия должен быть зафиксирован с использованием видеозаписи.

Перед началом ***осмотра средств компьютерной техники*** следователь должен определить для себя следующий важный момент: достаточно ли у него практических навыков, технических знаний для проведения осмотра того или иного носителя компьютерной информации и поиска доказательств, поскольку это трудоемкий процесс, требующий обладания специальными знаниями в области компьютерной техники, программного обеспечения. При отсутствии достаточных знаний, практического опыта следователь должен привлечь к участию в осмотре специалиста в данной области, чтобы вся имеющая доказательственное значение информация была обнаружена и зафиксирована. При этом следует учесть, что осмотр средств компьютерной техники по преступлениям в сфере высоких технологий является одним из основных следственных действий и его производство не терпит отлагательства. Конечно, идеальный вариант, когда осмотр средств компьютерной техники проводит сам следователь, который как никто иной (в том числе специалист) досконально знает материалы уголовного дела (следственную картину), в связи с чем может определить ту или иную обнаруженную информацию как относящуюся к делу (предмету доказывания) либо как не относящуюся к делу и не заслуживающую внимания. При этом в ходе осмотра при недостаточности практического опыта и технических знаний следователь должен в полной мере использовать иные источники: советы более опытных коллег, ресурсы сети Интернет, различную методическую литературу по данной тематике.

Согласно ст. 62 УПК специалистом является не заинтересованное в исходе уголовного дела лицо, обладающее специальными знаниями в науке, технике, искусстве, ремесле и иных сферах деятельности, вызванное органом, ведущим уголовный процесс, для участия и оказания содействия в производстве следственных и других процессуальных действий. При привлечении лица в качестве специалиста для участия в осмотре средств компьютерной техники следователь должен убедиться в специальной квалификации и профессиональном опыте лица путем проверки подтверждающих документов (например, диплома об окончании профильного учреждения профессионально-технического или высшего образования, трудовой книжки). Заверенные следователем копии таких документов необходимо приобщить к протоколу осмотра.

На практике к участию в проведении наиболее сложных с технической стороны осмотров средств компьютерной техники следователи управления по расследованию преступлений против информационной безопасности и интеллектуальной собственности главного следственного управления Следственного комитета Республики Беларусь в качестве специалистов привлекают сотрудников управления по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь с профильным образованием. Такие же специалисты проходят службу в областных подразделениях управления по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь и по согласованию с их непосредственными руководителями могут привлекаться для участия в осмотрах компьютерной техники следователями территориальных подразделений Следственного комитета.

Кроме того, в качестве специалистов могут быть привлечены любые иные лица, образование, квалификация и опыт работы которых соответствуют требованиям ст. 62 УПК, например сотрудники экспертных учреждений, учащиеся или выпускники профильных учреждений профессионально-технического или высшего образования.

В условиях недостаточности имеющихся в распоряжении следователя средств и методов для осмотра того или иного устройства по делу необходимо назначать *компьютерно-техническую экспертизу* для проведения исследований с применением специальных знаний и специальной техники (например, для установления вредоносных функций

программы, восстановления удаленной информации, расшифровки зашифрованных файлов и т. д.). При этом на разрешение эксперта необходимо ставить грамотные исчерпывающие вопросы с предоставлением необходимых материалов уголовного дела для того, чтобы исследования проводились быстро и эффективно.

В начале *протокола осмотра средств компьютерной техники* указываются общие сведения:

– о месте, времени составления протокола;

– участвующих в ходе осмотра участниках административного процесса (например, специалист);

– краткие сведения о конфигурации служебного компьютера, который будет использоваться в ходе осмотра изъятых средств компьютерной техники;

– сведения о компьютерных программах (название, версия, краткое описание основных возможностей), которые будут использоваться в ходе осмотра;

– краткие сведения об осматриваемом предмете (название, серийный номер) и месте его изъятия. Далее проводится визуальный осмотр устройства, в ходе которого фиксируются: форма (квадратная, прямоугольная, круглая, овальная и т. д.), размер (ширина, длина, толщина), материал корпуса (металл, пластик и т. д.), цвет;

– название устройства, фирма-изготовитель, серийный номер, объем памяти и другие технические данные (если такие отражены на поверхности корпуса или на фабричных ярлыках осматриваемого устройства);

– способ подключения к компьютеру.

Далее проводится детальный осмотр содержащейся на осматриваемом носителе информации; указываются распечатанные приложения к протоколу осмотра (если имеются). В конце протокола осмотра рекомендуется изложить выводы о результатах его проведения, поскольку осмотры средств компьютерной техники в основном являются объемными, с детальным описанием произведенных действий по достижению конечного искомого результата. Протокол может занимать до нескольких томов. Кроме того, в конце протокола осмотра описывается способ упаковки осмотренного устройства (устройств).

После проведения осмотра средств компьютерной техники протокол предъявляется для прочтения всем участникам, которые после ознакомления подписывают его. Замечания участников следственного действия подлежат внесению в протокол.

Если внешний вид устройства можно осмотреть визуально без применения специальной техники, то для осмотра информации, записанной на носителе, необходимо подключение к компьютеру.

В целях исключения возможности повреждения компьютерной информации при ее исследовании необходимо создать точную (побитовую) копию содержания машинного носителя информации, которая в последующем и будет использоваться при осмотре (исследовании), т. е. в дальнейшем сам машинный носитель с оригинальной информацией не используется, может быть упакован и сдан на хранение, что позволит сохранить и защитить как сам носитель, так и информацию, которые часто являются основными доказательствами по уголовному делу, от случайного повреждения или удаления.

В большинстве случаев следователи осматривают изъятые по делу носители машинной информации с использованием доступного программного обеспечения (например, программы Acronis True Image, которая предназначена для резервного копирования, восстановления данных, создания и управления образами логических дисков машинного носителя) и аппаратных средств (например, многофункциональный кабель IDE/SATA-to-USB, предназначенный для синхронизации с компьютером осматриваемых носителей информации (в частности, накопителей на жестких магнитных дисках) с распространенными интерфейсами подключения – IDE (Integrated Drive Electronics – параллельный интерфейс подключения накопителей), SATA (Serial Advanced Technology Attachment – последовательный интерфейс обмена данными)).

В любом случае при синхронизации осматриваемого машинного носителя информации со служебным компьютером следователь должен помнить основное правило: необходимо обеспечить сохранность исследуемой компьютерной информации, заблокировать любую возможность изменения (удаления) изначального состояния такой информации. На практике в следственных подразделениях для указанных целей используется программа WriteBlocker XP (предназначена для работы с операционной системой Windows XP, на операционной системе Windows-7 используется практически аналогичная программа Innovision-Forensics USB WriteBlocker). WriteBlocker XP предотвращает все намеренные, неумышленные и системно инициированные попытки записи на подключенные машинные носители информации, включая жесткие диски, гибкие диски и сменные диски, за исключением системного загрузочного диска, при этом позволяет просматривать и копировать информацию с таких носителей. WriteBlocker XP сохраняет блокированное (открытое) состояние на каждое присоединенное устройство после перезапуска системы. Достаточно установить данную программу на служебный компьютер, после чего она будет работать автоматически без каких-либо дополнительных настроек. Интерфейс программы WriteBlocker XP англоязычный, однако простой и удобный в использовании.

При проведении осмотра изъятого по уголовному делу машинного носителя компьютерной информации следует обеспечить безопасность не только вещественного доказательства, но также используемого для осмотра служебного компьютера и хранящейся на нем служебной информации, поскольку осматриваемые по компьютерным преступлениям устройства хранения информации ввиду специфики данного вида преступлений часто содержат различные вредоносные программы (компьютерные вирусы, троянские программы и т. д.), которые при проведении осмотра могут «заразить» служебный компьютер и в зависимости от вредоносной функции программы повлечь различного рода негативные последствия, вплоть до вывода из строя, блокирования или уничтожения служебного компьютерного оборудования либо удаления, изменения хранящейся на компьютере служебной информации. Для минимизации возможных негативных последствий на служебном компьютере должно быть установлено актуальное надежное антивирусное программное обеспечение с постоянным обновлением антивирусных баз.

После обеспечения сохранности осматриваемой информации, а также безопасности служебного компьютера и служебной информации можно осуществлять подключение изъятого по делу машинного носителя информации к служебному компьютеру для проведения осмотра его содержимого. Разные устройства хранения информации имеют различные способы синхронизации с компьютером. В практической деятельности используются следующие способы подключения носителей информации к компьютеру и специальные устройства:

– основным устройством хранения компьютерной информации является накопитель на жестких магнитных дисках. Его важным параметром служит используемая система обмена информацией между ним и материнской платой компьютера – так называемый интерфейс жесткого диска. Наиболее часто используемые интерфейсы – IDE и SATA;

– устройство внешний HDD синхронизируется с компьютером при помощи входящего в комплект поставки USB-кабеля;

– устройство Flash USB Drive не требует дополнительных средств для синхронизации с компьютером, поскольку само обладает интерфейсом USB (Universal Serial Bus – последовательный интерфейс передачи данных);

– для синхронизации с компьютером карты памяти Flash-memory необходимо специальное устройство чтения Card Reader;

– для чтения оптических (лазерных) дисков компьютер должен быть оборудован устройством чтения (записи) компакт-дисков (CD/DVD-дисководом).

– для синхронизации с компьютером карманных персональных компьютеров, мобильных телефонов, смартфонов, электронных книг,

MP3-плееров, цифровых фото- и видеокамер, GPS-навигаторов, игровых приставок и т. д. используются входящие в комплект поставки data-кабели или USB-кабели с соответствующим программным обеспечением (драйверами).

При производстве предварительного расследования следователь должен помнить следующий важный момент: осмотр машинных носителей компьютерной информации – основополагающее следственное действие как по компьютерным преступлениям, так и в некоторых случаях по иным преступлениям, к производству которого следует подходить ответственно, с использованием актуальных практических навыков, современных технических и программных средств. Следователю необходимо постоянно совершенствовать свои знания в сфере высоких технологий, программного обеспечения, способов совершения компьютерных преступлений, поскольку лица, совершающие преступления против информационной безопасности, всегда идут на несколько шагов впереди оперативных сотрудников и следователей, раскрывающих и расследующих такие преступления.

В *протоколе осмотра места происшествия* следует отразить следующие фактические данные:

– наименование и назначение объекта, где совершено преступление; его территориальное расположение (на улице, в помещении, банке, магазине, на автостоянке, бензоколонке, станции метро, в ресторане, гостинице, помещении кассы, на складе, вокзале, контрольно-пропускном пункте и т. д.) и его ориентацию относительно сторон света;

– ближайшее окружение объекта и подступы к нему (здания, технические сооружения, площади, зоны, участки (производственные, административные, жилые)) и расстояние до них; наличие дорог, подъездных путей (в том числе водного транспорта), парковок и автостоянок; наличие линий и пунктов (колодцы, концентраторы, коробы и т. д.) инженерно-технических коммуникаций (электросвязи, электропередачи, тепло-, водо- и газоснабжения, вентиляции и т. д.);

– технические и конструктивные особенности местности, связанные с установкой и эксплуатацией средств компьютерной техники (этажность, материал стен и других строительных конструкций, форма строения, наличие дверей, окон, ограждений, фальшполов и подвесных потолков, наличие и фактическое состояние устройств электропитания и т. д.);

– наличие, внешнее состояние и расположение охраны объекта, специальных защитных и сигнальных устройств от несанкционированного съема и утечки информации (посты охраны, охранно-пожарной сигнализации, контрольно-пропускных пунктов доступа лиц на данную тер-

риторию (неавтоматический, полуавтоматический или автоматический), освещение, металлические решетки, шторы, жалюзи, замки и запорные механизмы, экраны, заземления, специальные стекла и пленки, генераторы шума, фильтры и т. д.);

– расположение средств компьютерной техники относительно вентиляционных и иных отверстий в строительных конструкциях, дверных и оконных проемов, технических средств видеонаблюдения, а также других рабочих мест (если таковых несколько в одном помещении);

– расположение в одном помещении вместе со средствами компьютерной техники других электрических устройств и приборов (телефонные и иные аппараты электросвязи, оргтехника (копировальные аппараты, автоответчики и т. п.), приборы электроосвещения (настольные, напольные, настенные, потолочные, подвесные и т. д.), абонентские громкоговорители, телевизоры и мониторы, электроплитки, чайники, кондиционеры и т. д.);

– наличие в одном помещении со средствами компьютерной техники линий, пунктов, разъемов промежуточных и оконечных устройств систем инженерно-технических коммуникаций (электросвязи, электропередачи, антенны-провода, тепло-, водо- и газоснабжения);

– наличие или отсутствие технических средств сопряжения средств компьютерной техники с каналами электросвязи и между собой (на это могут указывать кабели и провода, которыми они соединены между собой, а также с аппаратами или линией электросвязи);

– наличие или отсутствие соединений средств компьютерной техники с оборудованием или вычислительной техникой, находящимися вне территории (помещения) осмотра (на это могут указывать кабели и провода, идущие от осматриваемого средства компьютерной техники за границу места осмотра (в другие помещения или здания) либо к аппаратам внутренней связи (в этом случае граница осмотра места происшествия значительно расширяется));

– наличие на объекте, путях подхода и отхода следов преступления и преступника (следы орудий взлома, повреждения, уничтожения и (или) модификации охранных и сигнальных устройств; показания регистрирующей (электронный журнал) или специальной мониторинговой (тестовой) аппаратуры; следы пальцев рук на средствах компьютерной техники, охранных и сигнальных устройствах, на их клавиатуре, соединительных и электропитающих проводах и разъемах, на розетках и штепсельных вилках, тумблерах, кнопках и рубильниках, включающих средства компьютерной техники и электрооборудование; остатки

соединительных проводов и изоляционных материалов, капли припоя, канифоли или флюса; следы проплавления, прокола, надреза изоляции проводов средств компьютерной техники, наличие участков механического сдавливания и приклеивания посторонних предметов);

– наличие или отсутствие учетно-справочной документации к средствам компьютерной техники (технический паспорт и подобный ему документ; журнал оператора или протокол автоматической фиксации расчетно-кассовых и иных операций; журнал учета машинных носителей информации, машинных документов, заказов (заданий или запросов); журнал (карточка) учета выдачи машинных носителей информации и машинных документов; журнал (карточка) учета массивов (участков, зон), программ, записанных на машинные носители информации; журнал учета уничтожения брака бумажных носителей информации и машинных документов; акты на стирание конфиденциальной информации, уничтожение машинных носителей с конфиденциальной информацией, конфиденциальных машинных документов).

Таким образом, осмотр места происшествия наряду с осмотром средств компьютерной техники является наиболее распространенным и одновременно наиболее важным следственным действием при расследовании преступлений в сфере высоких технологий. При проведении указанных видов осмотров добывается большинство доказательств как наличия самого общественно опасного деяния, так и вины подозреваемого.

4. ОРГАНИЗАЦИЯ РАССЛЕДОВАНИЯ НЕЗАКОННОГО РАСПРОСТРАНЕНИЯ ИЛИ ИНОГО НЕЗАКОННОГО ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНЫХ ПРОГРАММ КАК ОБЪЕКТОВ АВТОРСКОГО ПРАВА

Мировое сообщество на современном этапе придает большое значение вопросу организации защиты авторских, смежных прав и права промышленной собственности. Представители стран СНГ договорились о совместном противодействии нарушениям интеллектуального права, разработав перечень мероприятий в сфере противодействия правонарушениям в области интеллектуальной собственности.

Ситуацию на современном этапе в Республике Беларусь и меры, предпринимаемые органами уголовного преследования по борьбе с нарушениями авторских прав, рассмотрим на примере производства предварительного следствия по уголовным делам, когда объектом преступного посягательства является бухгалтерская программа «1С: Предприятие».

Анализ правоприменительной практики свидетельствует, что органы уголовного преследования Республики Беларусь осуществляют защиту в основном программных продуктов производителей других государств, представительства которых базируются на территории нашей страны. Наиболее ярким примером является бухгалтерская программа «1С: Предприятие», производитель которой – российская компания, расположенная в Москве. В Республике Беларусь имеется ряд ее представительств, действующих на основании доверенности. Они защищают на территории Республики Беларусь ее интересы как правообладателя. Если какая-либо организация или частный предприниматель (далее – лицо), имея право в рамках своей предпринимательской деятельности официально устанавливать распространяемые программы, захотят установить упомянутую программу («1С: Предприятие») или какую-либо другую лицензионную программу, они обязаны выяснить, кто является правообладателем, и затем обратиться к нему с целью заключения договора, дающего право на установку данной программы. Если же они предпримут попытку установки интересующей клиентов программы без договора правопреемника, то эти действия подпадают под состав преступления, предусмотренного ст. 201 УК, защищающей авторские, смежные права и права промышленной собственности.

Вместе с тем необходимо учитывать, что законодатель отнес эту норму к уголовным делам частно-публичного обвинения (ч. 4 ст. 26 УПК), которые возбуждаются только по заявлению лица, пострадавшего от преступления. Ч. 2 ст. 201 УК констатирует наличие административной преюдиции, что также следует иметь в виду при принятии решения о возбуждении уголовного дела. Как правило, представитель правообладателя программы на территории Республики Беларусь принимает меры по защите интересов стороны, которую он представляет. Для этого сотрудники представительства проводят аналитическую работу по обнаружению объявлений в сети Интернет или средствах массовой информации (рекламных газетах), что какое-то лицо устанавливает компьютерную программу, владельцем которой является их правообладатель. В связи с выявлением таких фактов они обращаются в органы внутренних дел с заявлением (сообщением) и просят провести проверку деятельности по установлению программного обеспечения конкретным лицом.

Обнаружение эпизодов преступной деятельности того или иного лица также возможно и оперативным путем. И если оперативные сотрудники выявляют такие эпизоды, то они обязаны согласовать свои действия в дальнейшем с представителем правообладателя и выяснить, желает ли он привлечь данное лицо к уголовной ответственности. Вместе с тем уголовно-процессуальный закон Республики Беларусь констатирует, что по таким преступлениям уголовное дело может быть возбуждено прокурором и при отсутствии заявления лица, пострадавшего от преступления, если имеется ряд условий, предусмотренных ч. 5 ст. 26 УПК.

С момента поступления заявления (сообщения) оперативный сотрудник приступает к проверке имеющейся в нем информации и начинает собирать доказательства, подтверждающие наличие оснований к возбуждению уголовного дела в соответствии с требованиями ч. 2 ст. 173 УПК. При этом возникают две ситуации:

1) в заявлении представитель правообладателя не только указывает лицо, устанавливающее контрафактные программы, но и приводит перечень организаций, где они установлены;

2) в заявлении (сообщении) речь идет только о распространителе контрафактного программного продукта.

С учетом данных ситуаций должна проводиться соответственно и проверка заявления (сообщения) оперативным сотрудником.

В первой ситуации в отношении установленного лица проводятся оперативно-розыскные мероприятия в соответствии с Законом Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности», а также процессуальные действия по проверке конкретных организаций на предмет подтверждения фактов установки конкретным лицом контрафактного программного продукта.

Во второй ситуации проводятся оперативно-розыскные мероприятия по установлению и документированию эпизодов преступной деятельности.

Как в первой, так и во второй ситуации деятельность в рамках предварительной проверки направлена на собирание доказательственной информации, указывающей на признаки преступления, предусмотренного ст. 201 УК. При этом наиболее важным моментом являются способы собирания доказательственной информации в конкретных организациях, где, по убеждению сотрудника органа уголовного преследования, установлены контрафактные программы.

В связи с тем что ч. 1 ст. 103 УПК констатирует возможность собирания доказательств в процессе разрешения заявлений и сообщений о преступлении, оперативный сотрудник вправе получить объяснения у работников организации о том, имеются ли аппаратный ключ защиты правообладателя и документы на приобретение данной программы. Как следует из практики, у владельца контрафактной программы отсутствует аппаратный ключ защиты, с помощью которого она запускается. Лицо, которое устанавливает контрафактную программу заказчику с помощью вирусных программ, или самостоятельно вносит изменения в лицензионную программу (эти изменения связаны со взломом ее аппаратного ключа либо его обходом), или приобретает готовую контрафактную программу. При получении объяснения необходимо выяснить, кто и когда устанавливал контрафактную программу, каким образом проводился расчет с лицом. Руководствуясь ч. 2 ст. 103 и ч. 2 ст. 173 УПК, следует истребовать как документы, подтверждающие приобретение установленной программы (договор купли-продажи, акт выполненных работ), так и документы, свидетельствующие об оплате лицу услуг по ее установке (платежные бухгалтерские документы).

Наряду с истребованием документов и получением объяснений в соответствии с ч. 1 ст. 103 УПК собирание доказательственной информации производится и в процессе проведения осмотра. Для того чтобы результаты осмотра отвечали требованиям ст. 105 УПК, оперативный сотрудник обязан провести осмотр места происшествия, руководствуясь требованиями ч. 2 ст. 173, ст. 203, 204 УПК, в рамках которого обследовать конкретные средства компьютерной техники и убедиться, что

программы, установленные на них, являются контрафактными. Наряду с требованиями процессуального закона следует также учитывать и тактический аспект производства данного следственного действия, а именно:

– необходимо провести осмотр помещения, где находятся средства компьютерной техники;

– последовательно осуществить осмотр каждого средства компьютерной техники.

При *визуальном осмотре конкретного компьютера* фиксируются: форма, размер, материал корпуса, цвет, название, фирма-изготовитель, серийный номер, объем памяти и другие технические данные, наличие на мониторе ярлыка или файла запуска программы. Если программа запускается, то отмечается отсутствие аппаратного ключа защиты в USB- или LTP-разъемах системного блока (LTP – Line Print Terminal – параллельный порт подключения периферийных устройств), что свидетельствует о явном признаке ее контрафактности (если установлена локальная версия программного обеспечения). На признак контрафактности установленной программы указывает также наличие нелицензионного драйвера ключа защиты (эмулятора ключа). Отмеченные признаки являются несомненным основанием для изъятия накопителя на жестких магнитных дисках осматриваемого компьютера с целью его последующего детального осмотра в органе уголовного преследования.

В ходе осмотра средств компьютерной техники может возникнуть ситуация, когда у организации имеются договор с аттестованным на территории Республики Беларусь продавцом лицензионного программного продукта, приобретенный диск с лицензионной программой и аппаратный ключ защиты для ее запуска, однако наряду с лицензионной программой на рабочих компьютерах установлена и контрафактная программа, что объясняется необходимостью использования конкретной программы данной организацией на нескольких машинных носителях информации в различных структурных подразделениях. Как правило, версия лицензионной программы рассчитана на установку на один или несколько компьютеров, при этом стоимость в одном и другом случае значительно отличается, поэтому организация, чтобы избежать дополнительных затрат и в то же время обезопасить себя, закупает одну однопользовательскую версию и устанавливает ее на один компьютер, а на остальные компьютеры – контрафактные программы.

После завершения осмотра *изымается накопитель на жестких магнитных дисках компьютера*, на котором установлена программа, имеющая признаки контрафактности, о чем делается отметка в протоколе. В случае если имеется информация о наличии контрафактных программ

на машинных носителях информации ряда организаций (следственная практика знает прецеденты, когда в поле зрения органов уголовного преследования попадало до 40 организаций, на компьютерной технике которых был установлен контрафактный программный продукт), то оперативный сотрудник обязан осуществить осмотр и изъятие накопителей на жестких магнитных дисках с учетом складывающейся ситуации в ходе проведения проверки, чтобы не допустить их уничтожения работниками этих организаций. Если нет реальной возможности изъятия компьютерной техники из-за технологического процесса организации, то целесообразно создать образ памяти информации с накопителя на жестких магнитных дисках. Однако такое решение может быть принято только следователем при производстве расследования по конкретному уголовному делу в соответствии с требованиями ст. 96, 97 УПК. Оперативный сотрудник обязан собрать доказательства, указывающие на признаки преступления, предусмотренного ч. 2 или 3 ст. 201 УК, и представить подлинные источники доказательств следователю для принятия решения о возбуждении уголовного дела.

После изъятия накопителя на жестких магнитных дисках сотрудник органа уголовного преследования обязан незамедлительно назначить экспертизу, для того чтобы эксперт установил, действительно ли на нем имеется программа, обладающая признаками контрафактности. Согласно букве закона *производство компьютерно-технической экспертизы* поручается соответствующим подразделениям Государственного комитета судебных экспертиз Республики Беларусь (ст. 230 УПК), также данная экспертиза может быть проведена и вне экспертного учреждения, а именно ее производство поручено компетентному специалисту в области программного обеспечения (ст. 231 УПК).

При этом не следует поручать проведение данной экспертизы специалистам представителя правообладателя, обратившегося с заявлением о распространении контрафактных программ, или другого представительства, у которых есть копии лицензионных программ и их сотрудники имеют реальную возможность установления идентификационного тождества или отсутствия такового между программными продуктами, поскольку в ходе производства предварительного следствия защитник, представляющий интересы обвиняемого, будет заявлять ходатайства, констатируя заинтересованность должностных лиц данного представительства, и тем самым предпримет попытку поставить под сомнение заключение эксперта, которое подготовят специалисты представителя.

При назначении экспертизы оперативный сотрудник в постановлении формулирует ряд вопросов, разрешение которых экспертом позволит

определить, установлена ли на изъятом и представленном на исследование накопителе на жестких магнитных дисках контрафактная программа:

– имеются ли на представленном на исследование машинном носителе информации воспроизведенные и инсталлированные (установленные) компьютерные программы комплекса «1С: Предприятие»; какие версии компьютерной программы комплекса «1С: Предприятие» установлены на представленном на исследование машинном носителе информации, работоспособны ли они;

– какая информация о времени установки и использования компьютерной программы комплекса «1С: Предприятие» имеется на представленном на исследование машинном носителе информации;

– имеются ли на машинном носителе информации программы, предназначенные для удаления и блокирования средств защиты компьютерной программы комплекса «1С: Предприятие» от несанкционированного использования и копирования; если да, то каков механизм их действия и последствия применения;

– имеются ли следы использования программ для удаления, блокирования и модификации компьютерной программы комплекса «1С: Предприятие» на представленном на исследование машинном носителе информации; какие изменения были произведены в компьютерной программе?

В ходе проверки также следует выяснить факт правообладания лицензионным компьютерным программным продуктом и стоимость лицензионной компьютерной программы.

Ч. 2 ст. 103 УПК предоставляет право органу уголовного преследования по собственной инициативе по находящимся в производстве материалам и уголовным делам требовать от организаций, должностных лиц представления предметов и документов, имеющих значение для уголовного дела. В этой связи оперативный сотрудник, руководствуясь данной нормой, обязан истребовать у правообладателя документы, подтверждающие факт правомерности владения лицензионным программным продуктом, а также документы, подтверждающие стоимость лицензионной компьютерной программы. Последние необходимы для установления размера вреда, причиненного в результате совершения преступных действий по распространению контрафактного программного продукта.

Собрав доказательственную информацию о преступных действиях конкретного лица по распространению контрафактного программного продукта, орган дознания, руководствуясь требованиями ст. 174–177, 186 УПК, возбуждает уголовное дело и производит неотложные следственные и другие процессуальные действия для установления и закрепления следов преступления и после их выполнения передает дело сле-

дователю или направляет материалы проверки следователю, который при наличии в них признаков преступления, предусмотренного ч. 2, 3 ст. 201 УК, принимает решение о возбуждении уголовного дела либо требует провести дополнительные процессуальные действия для выяснения отдельных неустановленных обстоятельств.

При проведении проверочных действий по заявлению (сообщению) о преступлении, предусмотренном ст. 201 УК, сотрудник органа уголовного преследования обязан:

– выяснить, в каких организациях установлен контрафактный программный продукт;

– произвести осмотр средств компьютерной техники и изъятие накопителя на жестких магнитных дисках с имеющимся на них программным продуктом, обладающим признаками контрафактности;

– назначить компьютерно-техническую экспертизу изъятых накопителей на жестких магнитных дисках;

– получить объяснения у работников организаций о фактах установления контрафактного программного продукта;

– истребовать у должностных лиц, организаций документы, подтверждающие обстоятельства установления контрафактного программного продукта и порядок расчета с лицом, его установившим;

– выяснить размер дохода и ущерба в соответствии с требованиями ч. 2, 3 ст. 201 УК;

– проверить правомерность правообладания компьютерным программным продуктом.

Организация работы следователя в большей мере зависит от конкретно складывающейся следственной ситуации по переданным материалам или возбужденному уголовному делу и сводится к планированию следственных и других процессуальных действий с целью получения новых доказательств, позволяющих всесторонне, полно и объективно установить обстоятельства, подлежащие доказыванию в соответствии с конструкцией ст. 201 УК, а также к принятию конкретных процессуальных решений.

В этой связи следователь и оперативный сотрудник обязаны незамедлительно запланировать и провести следующие следственные и другие процессуальные действия:

– выемку накопителя на жестких магнитных дисках, на котором установлен контрафактный программный продукт в конкретной организации, если изъятие не проводилось на всех объектах оперативными сотрудниками;

– осмотр изъятого накопителя на жестких магнитных дисках или его копии;

– назначение компьютерно-технической экспертизы изъятого накопителя на жестких магнитных дисках;

– допрос работника организации, заключавшего договор на приобретение и установку контрафактного программного продукта;

– допросы работников организации, на служебных компьютерах которых установлен контрафактный программный продукт;

– выемку договора и финансовых документов, удостоверяющих оплату приобретенного контрафактного программного продукта и его установку;

– задержание и допрос подозреваемого;

– обыск по месту жительства и работы подозреваемого;

– расчет объема ущерба с учетом количества доказанных эпизодов преступной деятельности;

– вынесение постановления о привлечении в качестве обвиняемого, предъявление обвинения, допрос обвиняемого.

Среди условно выделенных следственных и других процессуальных действий в алгоритме расследования рассматриваемого преступления необходимо учитывать особенности производства выемки накопителя на жестких магнитных дисках в организации. Принимая решение о производстве выемки, следователю необходимо изучить место ее проведения. В следственной практике органов уголовного преследования имеют место случаи, когда организация зарегистрирована по одному юридическому адресу, а деятельность осуществляет по другому. Данный аспект следует учитывать при составлении процессуальных документов о производстве выемки. В организации целесообразно обратить внимание на количество средств компьютерной техники, на которых, возможно, установлен контрафактный программный продукт. Следует иметь в виду, что в большинстве случаев контрафактная компьютерная программа «1С: Предприятие» устанавливается на всех компьютерах бухгалтерского отдела, в связи с чем изъятие всех накопителей на жестких магнитных дисках, на которых она инсталлирована, может иметь негативные последствия для нормального функционирования организации. Для того чтобы не возник конфликт с представителями организации, практические сотрудники поступают следующим образом. Органу дознания дается поручение о производстве выемки и осмотра накопителя на жестких магнитных дисках. В поручении следователь отражает, что должен сделать оперативный сотрудник:

– изъять накопитель на жестких магнитных дисках;

– осмотреть накопитель на жестких магнитных дисках, создав образ памяти интересующей информации с него либо полную копию накопителя на жестких магнитных дисках, поместить образ памяти созданной

информации на служебный компьютер, иной машинный носитель информации. В ходе осмотра оперативный сотрудник должен применять специальное программное обеспечение, исключающее намеренное и случайное изменение (удаление) информации, хранящейся на осматриваемом накопителе на жестких магнитных дисках;

– подсчитать контрольную сумму созданной копии (она отражает объем информации, хранящейся на накопителе на жестких магнитных дисках);

– возвратить накопитель на жестких магнитных дисках должностному лицу организации для хранения до вступления приговора суда в законную силу.

Подсчет контрольной суммы оперативный сотрудник обязан осуществить для того, чтобы у участников процесса не возникло впоследствии сомнений по поводу того, что, возможно, были внесены изменения в содержание информации, хранящейся на изымаемом накопителе на жестких магнитных дисках, при создании его копии. Контрольная сумма, состоящая из 30 цифр и букв, подтверждает первоначальное содержание скопированной информации. Если в дальнейшем, при производстве предварительного следствия, в ходе осмотра следователем копии информации с накопителя на жестких магнитных дисках при подсчете данная контрольная сумма не будет совпадать с первоначально зафиксированной в ходе его изъятия оперативным сотрудником, данное обстоятельство может повлечь заявление ходатайств со стороны защиты, что были внесены изменения в копию информации с накопителя на жестких магнитных дисках.

В соответствии с требованиями ст. 210 и 212 УПК оперативный сотрудник производит выемку накопителя на жестких магнитных дисках с установленной на нем компьютерной программой, имеющей признаки контрафактности, осматривает его и изготавливает копию информации с него. Копия переносится на служебный компьютер, имеющийся у оперативного сотрудника, и затем он возвращает законному владельцу (представителю администрации организации) накопитель на жестких магнитных дисках и разъясняет необходимость сохранения имеющейся на нем компьютерной программы, имеющей признаки контрафактности.

Как следует из практики, факт передачи накопителя на жестких магнитных дисках представителю организации фиксируется в акте передачи на хранение накопителя на жестких магнитных дисках и в его содержании констатируется, что накопитель на жестких магнитных дисках является вещественным доказательством по уголовному делу, а работник, которому он передается, предупреждается об уголовной ответственности за его утрату либо отчуждение в соответствии со ст. 409 УК. В прак-

тической деятельности имеют место случаи, когда следователь готовит данный акт от своего имени и прилагает к поручению, направляемому органу дознания, а исполнитель – оперативный сотрудник – впоследствии от его имени осуществляет передачу изъятого и осмотренного накопителя на жестких магнитных дисках. Однако указанные действия неправомерны, поскольку:

– если оперативный сотрудник выполняет поручение следователя, то все процессуальные действия в рамках изложенного поручения должны производиться им непосредственно, а не от имени следователя, так как доказательство должно быть получено в установленном законом порядке и отвечать требованию допустимости;

– процессуальная форма самого акта как процессуального документа не предусмотрена действующим УПК;

– право констатировать на момент производства выемки статус накопителя на жестких магнитных дисках с инсталлированным на нем контрафактным программным продуктом как «вещественное доказательство» принадлежит исключительно следователю, осуществляющему производство по уголовному делу, и принимается такое решение после осмотра им копии информации с накопителя на жестких магнитных дисках, представленной оперативным сотрудником.

Следовательно, выработанный практикой механизм собирания доказательств при производстве выемки по рассматриваемой категории преступлений не является бесспорным. С одной стороны, он позволяет не допустить нарушения производственного процесса предприятия, что является разумным и правомерным, с другой – ставит под сомнение процессуальный статус изъятого накопителя на жестких магнитных дисках в качестве вещественного доказательства по уголовному делу. Действующие уголовно-процессуальные нормы на первый взгляд не позволяют следователю в описанной ситуации найти более правильный механизм действий по получению доказательственной информации. Выход из имеющей место практической ситуации видится в следующем. Следователь может лично провести выемку в организации, осуществить осмотр накопителя на жестких магнитных дисках и изготовить образ памяти информации с него, признать его вещественным доказательством и передать на хранение работнику органинизации. Однако с позиции осуществления расследования по уголовному делу это не всегда является оправданным и целесообразным, так как передача накопителя на жестких магнитных дисках может привести к невозможности соблюдения требований ст. 337 УПК судом, который обязан непосредственно исследовать с участием сторон сами вещественные до-

казательства (первичный объект – машинный носитель информации) по рассматриваемому уголовному делу, а не сведения о них, содержащиеся в протоколе проведенного следователем осмотра служебного компьютера оперативного сотрудника, на котором он представил ему копию контрафактной программы. В связи с этим наиболее правильным будет являться выемка накопителя на жестких магнитных дисках, на котором инсталлирован контрафактный программный продукт, непосредственно следователем или дача им поручения органу дознания о производстве данного следственного действия. Обусловлено это тем, что, если накопитель на жестких магнитных дисках останется в организации, возможна ситуация, когда несанкционированный доступ к компьютерной информации, компьютерный саботаж, использование вредоносных программ, технические неисправности средств компьютерной техники могут повлечь утрату контрафактного программного продукта помимо воли должностного лица.

Следует отметить, что практика производства расследования преступлений против интеллектуальной собственности, когда объектом преступления является программный продукт, до настоящего времени не знала прецедентов уничтожения или внесения изменений работниками организации в переданный им на хранение накопитель на жестких магнитных дисках с инсталлированным контрафактным программным продуктом. В некоторой мере такая ситуация обусловлена сложностью доказывания в их действиях прямого умысла на незаконное использование контрафактного программного продукта в производственном процессе, и они данное обстоятельство прекрасно осознают и поэтому не предпринимают никаких противоправных действий. Сдерживающим фактором для внесения изменений или уничтожения контрафактного программного продукта является также то обстоятельство, что в протоколе выемки оперативный сотрудник в обязательном порядке фиксирует факт изготовления копии информации с осматриваемого накопителя на жестких магнитных дисках и передачи его законному владельцу, а также требование о сохранении имеющейся информации в том состоянии, которое было на момент осмотра объекта. Немаловажным обстоятельством является также приглашение для производства выемки накопителя на жестких магнитных дисках с установленным на нем контрафактным программным продуктом таких участников процесса, как понятые, хотя действующий уголовно-процессуальный закон прямо не указывает на их участие. В случае возникновения в последующем ситуации, связанной с утратой контрафактного программного продукта, последние должны быть допрошены в качестве свидетелей как в ходе производства предварительного следствия, так и в судебном разбирательстве.

При производстве выемки по уголовным делам рассматриваемой категории не следует пренебрегать положением ч. 15 ст. 210 УПК, согласно которой следователь, оперативный сотрудник обязаны разъяснить должностному лицу администрации организации право изготовить копии с изъятых документов и иных носителей информации. Об изготовлении копий и соответствии их изымаемым подлинникам производится отметка в протоколе выемки. Данное положение закона позволяет должностному лицу администрации организации, где производится выемка накопителя на жестких магнитных дисках с установленным контрафактным программным продуктом, изготовить копию этого программного продукта с соблюдением требований отмеченной уголовно-процессуальной нормы.

В ходе расследования следователь в зависимости от сложившейся следственной ситуации по уголовному делу производит *осмотр изъятого накопителя на жестких магнитных дисках или образа памяти информации с него*. Осмотр накопителя на жестких магнитных дисках имеет место в случаях, если последний поступил с материалами проверки из органа дознания или изъят при производстве обыска либо выемки как органом дознания в процессе исполнения поручения следователя, так и непосредственно следователем в ходе производства следственных действий. Осмотр образа памяти информации с накопителя на жестких магнитных дисках производится в том случае, когда он изготовлен оперативным сотрудником в ходе выполнения поручения следователя и передан ему на служебном компьютере, ином машинном носителе информации.

При проведении осмотра необходимо придерживаться ряда правил, выработанных следственной практикой.

Особенность осмотра любой компьютерной техники заключается в том, что нельзя подключать изъятый накопитель на жестких магнитных дисках к своему служебному компьютеру и начинать осмотр, поскольку при включении компьютера сразу же вносятся изменения в реестр данных операционной системы и потом невозможно использовать сам накопитель на жестких магнитных дисках и хранящуюся на нем информацию в качестве доказательств. Вследствие этого в ходе производства по уголовному делу защитник может заявить ходатайство о том, что после изъятия на накопитель на жестких магнитных дисках были внесены изменения, а именно следователь мог самостоятельно установить контрафактную программу, а не подозреваемый (обвиняемый). В связи с этим, прежде чем приступить к осмотру, следователь запускает на своем служебном компьютере программу или программно-аппаратный комплекс, позволяющие проводить исследования без внесения каких-либо изменений в объект осмотра. В частности, в практической деятельности ор-

ганов уголовного преследования применяется программно-аппаратный комплекс EnCase, который дает возможность не только просматривать, но и копировать информацию, находящуюся на осматриваемом накопителе на жестких магнитных дисках. В большинстве случаев следователи осматривают изъятые по делу машинные носители информации с использованием доступного программного обеспечения и аппаратных средств. В следственных подразделениях для указанных целей используется программа WriteBlocker XP.

Использование блокировочных программ или аппаратных средств дает возможность сохранить находящуюся на изъятом накопителе на жестких магнитных дисках информацию в первоначальном виде, что позволит впоследствии оперировать ею при доказывании вины лица как в ходе предварительного следствия, так и в судебном заседании.

Осмотр изъятого накопителя на жестких магнитных дисках без применения блокировочных программ или аппаратных средств влечет потерю доказательственной информации, что, в свою очередь, приводит к исключению протокола осмотра накопителя на жестких магнитных дисках, а также осмотренного вещественного доказательства (накопителя на жестких магнитных дисках) из системы доказательств по конкретному уголовному делу.

Для того чтобы избежать повреждения компьютерной информации при ее исследовании, создается образ памяти содержания машинного носителя информации, который в последующем и будет использоваться при осмотре. В дальнейшем сам машинный носитель информации с оригинальной информацией не используется, он упаковывается и сдается на хранение, что позволяет сохранить и защитить как носитель, так и информацию, которая часто является основным доказательством по уголовному делу, от случайного повреждения или удаления. Осмотр образа памяти программного продукта «1С: Предприятие» может производиться без блокирующего устройства, и если не сформирована ошибка о запуске программы и она запускается без аппаратного ключа, то данное обстоятельство свидетельствует о том, что она является контрафактной, так как в лицензионной программе обязательно используется ключ защиты.

Используя программы для осмотра реестра Windows, содержащего информацию о том, какие действия и манипуляции проводились с компьютером, следователь определяет: когда устанавливалась контрафактная программа, какой пользователь ее установил, когда она запускалась, какие драйверы установлены.

Следует иметь в виду, что лицензионная программа имеет лицензионный драйвер. В процессе функционирования лицензионная программа

«1С: Предприятие» обращается к своему драйверу аппаратного ключа защиты. В процессе запуска лицензионный драйвер обращается к аппаратному ключу и, установив его наличие на компьютере, дает команду на запуск основной программы. В контрафактной программе удаляется лицензионный драйвер и вместо него подозреваемый устанавливает свой драйвер, который обрабатывает всю информацию, передаваемую основной программой, симулирует наличие аппаратного ключа и разрешает тем самым запуск программы. На самом деле аппаратный ключ защиты отсутствует. Осматривая драйвер, следователь видит, что программа запускается, однако он не лицензионный, о чем свидетельствуют свойства драйвера, вид, размер, дата установки, а также информация о его изготовителе. Обычно в программе «1С: Предприятие» в свойствах драйвера имеется отметка «1С: Предприятие» или «Аладдин». Контрафактный драйвер является своего рода вредоносной программой, и, как свидетельствует следственная практика, данные обозначения в свойствах такого драйвера отсутствуют или имеется маркировка Sable.

Для проведения осмотра копии информации с накопителя на жестких магнитных дисках, изготовленной оперативным сотрудником в ходе выполнения поручения следователя, вместе с рапортом о результатах проделанной работы, к которому приобщаются процессуальные документы, подтверждающие результаты производства выемки и осмотра накопителя на жестких магнитных дисках, следователю передается служебный компьютер (иной машинный носитель информации), на котором хранится копия изготовленного контрафактного программного продукта, о чем имеется отметка в рапорте. Получив служебный компьютер, следователь производит его осмотр, в ходе которого отражает, в какой папке хранится образ памяти информации с накопителя на жестких магнитных дисках, оговаривает в протоколе, что копирует ее и переносит на свой служебный компьютер.

Перед началом осмотра следователь подсчитывает контрольную сумму (отражает объем информации, хранящейся на копии информации с накопителя на жестких магнитных дисках) и фиксирует ее в протоколе осмотра. Она должна совпадать с суммой, которую зафиксировал оперативный сотрудник на момент осмотра накопителя на жестких магнитных дисках в организации, т. е. констатируется факт, что с момента изъятия образа памяти информации с накопителя на жестких магнитных дисках и передачи ее следователю какие-либо изменения с информацией не производились. После этого следователь проводит осмотр образа памяти информации с накопителя на жестких магнитных дисках и затем вновь производит подсчет контрольной суммы, которая должна соответ-

ствовать предыдущим (на момент изъятия оперативным сотрудником, на момент начала осмотра следователем и на момент окончания осмотра следователем).

Если объем образа памяти информации с накопителя на жестких магнитных дисках небольшой, то следователь записывает ее на внешний носитель информации и прилагает к протоколу осмотра, делая оговорку об этом в самом протоколе.

Если же объем информации значительный (в практической деятельности фигурируют объемы информации в 500 гигабайт и более), то образ памяти информации с накопителя на жестких магнитных дисках хранится на служебном компьютере следователя до принятия решения судом, который в приговоре определит ее судьбу. Следователю суд высылает копию приговора или направляет уведомление, содержащее распоряжение о судьбе хранящейся у него по конкретному уголовному делу информации. Следует иметь в виду, что в ходе судебного следствия у суда может возникнуть необходимость осмотреть хранящуюся у следователя информацию, поэтому он полномочен истребовать ее. В данной ситуации следователь обязан осуществить ее запись и передачу суду.

Результаты осмотра фиксируются следователем в соответствии с правилами ст. 193 УПК в *протоколе следственного действия*. Наряду с общими требованиями во вводной части должны быть зафиксированы сведения:

– о конфигурации служебного компьютера, который будет использоваться в ходе осмотра изъятых средств компьютерной техники;

– о компьютерных программах (название, версия, краткое описание основных возможностей), которые будут использоваться в ходе осмотра;

– краткие сведения об осматриваемом предмете (название, серийный номер) и месте его изъятия, а также результаты визуального осмотра накопителя на жестких магнитных дисках (форма, размер, материал корпуса, цвет; название, фирма-изготовитель, серийный номер, объем памяти и другие технические данные (если такие отражены на поверхности корпуса или на фабричных ярлыках); способ подключения к компьютеру).

В описательной части протокола следователь поэтапно отражает, какие логические разделы имеются на изъятом накопителе на жестких магнитных дисках. Кроме того, он должен создать снимки экрана своего служебного компьютера, когда на нем появляется информация после применения той или иной из используемых им компьютерных программ в ходе осмотра.

Нередко следователи после завершения следственного действия в процессуальном документе констатируют факт, что на осматриваемом накопителе на жестких магнитных дисках инсталлирована компьютерная программа, имеющая признаки контрафактности. Фактически действия следователя по осмотру изъятого накопителя на жестких магнитных дисках с контрафактной программой сходны по своей природе с действиями эксперта, проводящего экспертизу по конкретной экспертной методике.

С учетом количества изъятых накопителей на жестких магнитных дисках будет соответственно проведено и количество их осмотров, за исключением одного, по которому назначается экспертиза. Необходимо заметить, что осмотр изъятого накопителя на жестких магнитных дисках может длиться от трех-четырех дней до одного месяца, хорошо подготовленный следователь (в совершенстве владеющий программным обеспечением и методикой проведения осмотра) осуществляет осмотр в течение двух-трех суток.

Проведение осмотра помогает следователю сократить сроки производства экспертиз по уголовному делу и тем самым позволяет в некоторой мере сократить сроки производства расследования по уголовному делу в целом.

Оперативные сотрудники назначают экспертизу только по одному эпизоду в тех случаях, если установка производилась одним или несколькими подозреваемыми на ряде объектов, и при категоричном заключении эксперта передают материалы следователю для принятия решения о возбуждении уголовного дела. В ходе расследования в зависимости от складывающейся следственной ситуации и имеющейся совокупности доказательств следователь принимает решение о назначении экспертиз по другим преступным эпизодам.

Следующий этап осмотра изъятого накопителя на жестких магнитных дисках – привлечение к осмотру в качестве специалиста оперативного сотрудника из оперативного подразделения по раскрытию преступлений в сфере высоких технологий. В штат данных подразделений наряду с оперативными сотрудниками, имеющими юридическое образование, включены сотрудники, имеющие техническое образование, как правило, это оперативные сотрудники-программисты. Они обладают специальными знаниями в области компьютерной техники и программного обеспечения, поэтому следователи привлекают их к проведению осмотров в качестве специалистов.

Важным моментом в деятельности следователя является оценка результатов осмотра накопителя на жестких магнитных дисках судом при рассмотрении уголовного дела и принятии решения по нему. В ходе судебного разбирательства результаты осмотра изъятого накопителя на жестких магнитных дисках оцениваются как доказательства по уголовному делу и являются допустимыми при постановлении приговора. В случае если у суда возникнут сомнения по поводу проведенного следователем осмотра по отдельным эпизодам, он может назначить компьютерно-техническую экспертизу.

Одним из существенных моментов при производстве расследования рассматриваемого вида преступления является организация *допроса должностного лица организации, заключавшего договор на приобретение и установку компьютерного программного продукта*, оценка его показаний и использование последних в процессе доказывания виновности лица, распространявшего контрафактный программный продукт. В соответствии с требованиями ч. 2 ст. 94 УПК в ходе допроса следователь должен выяснить:

– какими обстоятельствами была вызвана необходимость установки программного продукта в организации;

– какие предварительные (подготовительные) действия должностных лиц, в обязанности которых входило приобретение товарно-материальных ценностей для организации, предшествовали установлению контрафактного программного продукта.

Определяя, какие предварительные действия предшествовали установлению программного продукта, следователь должен выяснить:

– проводился ли мониторинг рынка правообладателей, занимающихся распространением программного продукта на территории Республики Беларусь;

– объявлялся ли тендер на приобретение программного продукта;

– каковы условия и порядок его проведения;

– соответствовало ли его реальное проведение требованиям нормативно-правового порядка;

– если тендер был проведен, то кто его выиграл;

– когда был заключен с победителем тендера договор и на каких условиях;

– каковы договорные условия расчета за поставленную программную продукцию и как реально производился расчет;

– когда был установлен программный продукт в организации и на машинные носители информации каких структурных подразделений;

– кто осуществлял непосредственную установку программного продукта;

– какая техническая документация была представлена для его гарантийного сервисного обслуживания и на каких условиях;

– производилось ли его обслуживание.

При проведении допроса следователь должен учитывать следующие обстоятельства. При поставке программного продукта продавец обязан передать покупателю инструкцию по пользованию программным продуктом или техническое описание последнего. Следует иметь в виду, что в зависимости от вида программного продукта должна быть передана соответствующая техническая документация и это обстоятельство

должно быть отражено в договоре купли-продажи. Обслуживание реализованного программного продукта может осуществляться постоянно (до одного года) или по вызову специалистами компании-продавца. Это обстоятельство может быть также отражено в договоре на приобретение программного продукта. В договоре покупатель также может формулировать требование об обучении персонала работе с приобретенным программным продуктом. Следовательно, необходимо выяснить, кто из работников организации (технический специалист в области программного обеспечения) отвечал за качественное функционирование приобретенного программного продукта.

В условиях быстро развивающегося технического прогресса не следует исключать и ситуацию, что программный продукт приобретен на электронных торгах. В связи с этим полученные в ходе допроса показания должны быть проверены в Национальном центре маркетинга и конъюнктуры цен.

В ходе расследования может возникнуть следственная ситуация, когда тендер на закупку программной продукции вообще не проводился, а ее установка выполнялась в организации индивидуальным предпринимателем или вообще иным частным лицом. В связи с этим предмет допроса и обстоятельства, подлежащие выяснению, будут отличаться от вышеизложенной ситуации. При этом следователь должен будет выяснить в процессе допроса следующие обстоятельства:

– если тендер не проводился, то кто осуществлял установку программного продукта и на каких условиях;

– каким образом должностное лицо организации получило информацию о деятельности данного лица по оказанию услуг, связанных с реализацией программного продукта;

– заключался ли договор на поставку программного продукта и на каких условиях;

– когда был установлен программный продукт и как производился расчет за его установку.

Как свидетельствует практика расследования преступлений рассматриваемой категории, при даче показаний должностные лица придерживаются классической версии: не знали о том, что приобретаемая ими для нужд организации компьютерная программа является контрафактной, а при ее приобретении руководствовались установкой «о необходимости приобрести товар дешевле» и действовали во благо интересов организации.

В ходе *допросов работников организации*, на служебных компьютерах которых установлен контрафактный программный продукт, следователь должен получить ответы на следующие вопросы:

– когда был установлен программный продукт на служебный компьютер и по указанию какого должностного лица организации;

– кто осуществлял установку компьютерной программы;

– знакомило ли лицо, осуществлявшее установку программы, с технической документацией по эксплуатации программного продукта или проводило обучение в качестве пользователя;

– как производилось сервисное обслуживание установленного программного продукта и на протяжении какого периода времени?

Наряду с допросами должностных лиц, заключивших договор на поставку программного продукта, и работников, осуществлявших его эксплуатацию, должны быть допрошены и работники бухгалтерии, осуществлявшие расчет в соответствии с договором, по следующим обстоятельствам:

– когда была произведена оплата за установку программного продукта и на каких условиях;

– соответствовали ли условия оплаты заключенному с юридическим лицом, индивидуальным предпринимателем или физическим лицом договору;

– какая сумма денежных средств перечислялась и на какой расчетный счет.

Доказывая виновность конкретного лица в совершении преступления, предусмотренного ст. 201 УК, следует помнить, что наряду с показаниями отмеченных участников уголовного процесса важное место в совокупности доказательств занимают протоколы выемки и осмотра, позволяющие удостоверить обстоятельства и факт заключения договора на приобретение, установку контрафактного программного продукта, а также его оплату покупателем. При производстве расследования по уголовному делу данные следственные действия в обязательном порядке должны быть запланированы и проведены. Наличие в материалах уголовного дела договора на приобретение, установку контрафактного программного продукта и финансовых документов об оплате за произведенную работу позволит следователю доказать объективную сторону ст. 201 УК, выразившуюся в незаконном его распространении.

В ряде случаев на отдельном этапе производства предварительного следствия для достижения какой-либо промежуточной цели расследования и решения поставленных задач возникает необходимость алгоритмизации расследования. Относительно рассматриваемого преступления это этап, связанный с доказыванием причастности лица, распространившего контрафактный программный продукт, и определением его процессуального статуса (подозреваемый, обвиняемый).

Результаты рассмотренных выше следственных действий (протоколы выемки накопителя на жестких магнитных дисках с инсталлированным контрафактным программным продуктом и его осмотра; заключение компьютерно-технической экспертизы последнего; протоколы выемки

договоров и финансовых документов на его приобретение и установку; показания работников организации, заключивших договор на приобретение контрафактного программного продукта; показания работников, на служебных компьютерах которых установлен контрафактный программный продукт) позволяют доказать причастность конкретного лица к распространению контрафактного программного продукта. Организуя и планируя работу, следователь определяет ту или иную последовательность производства следственных действий по уголовному делу. Сущность их производства очевидна, и последовательность проведения не сможет вызвать каких-либо отрицательных последствий для процесса расследования по уголовному делу в целом.

В алгоритме по доказыванию причастности конкретного лица к совершению рассматриваемого преступления важное место занимают принятие решения о признании его в качестве подозреваемого и проведение с участием последнего отдельных следственных действий – допроса подозреваемого и обысков по его месту жительства и работы. Применительно к категории рассматриваемых преступлений процессуальный статус подозреваемого лицо может приобрести во всех предусмотренных ч. 1 ст. 40 УПК случаях. При этом следует учитывать то обстоятельство, что *алгоритм расследования* будет иметь особенности в зависимости от складывающейся следственной ситуации:

1) лицо задержано в соответствии с требованиями ст. 108, 110 УПК при проведении проверки заявления или сообщения о преступлении в порядке ст. 173 УПК;

2) уголовное дело возбуждено органом дознания (следователем) в соответствии с ч. 1 ст. 175 УПК в отношении лица, подозреваемого в совершении преступления, или по факту его совершения;

3) в отношении лица вынесено постановление о признании подозреваемым или о применении меры пресечения до вынесения постановления о привлечении его в качестве обвиняемого.

В первой выделенной ситуации алгоритм расследования будет иметь особенности, связанные с ограничением в ходе проведения проверки производством только отдельных следственных и процессуальных действий, предусмотренных ч. 2 ст. 173 УПК.

Во второй следственной ситуации при условии возбуждения уголовного дела органом дознания алгоритм зависит от ограничений, предусмотренных правилами производства следственных и других процессуальных действий для установления и закрепления следов преступления, предусмотренных ч. 1 ст. 186 УПК. При возбуждении уголовного дела следователем алгоритмизация расследования приобретает более широкие возможности с учетом процессуального статуса последнего.

Алгоритм расследования в третьей следственной ситуации находится в прямой зависимости от процессуальных полномочий органа дознания или следователя, принявших решение о применении меры пресечения в отношении подозреваемого или о признании лица подозреваемым.

Принимая решение о признании лица подозреваемым и проведении его допроса, а также производстве обысков по месту жительства и работы подозреваемого, следует организовать их проведение одновременно или сначала запланировать производство обысков, а затем – вызов (задержание) и допрос подозреваемого.

В первом случае производство отмеченных процессуальных и следственных действий осуществляется одновременно следователем и сотрудниками органа дознания. При этом сотрудники органа дознания производят обыски по поручению следователя. Если уголовное дело находится в производстве органа дознания, то проведение отмеченных следственных действий осуществляет лицо, производящее дознание, и сотрудники органа дознания по его мотивированному ходатайству.

Во втором случае производство обысков может осуществляться как непосредственно следователем, так и лицом, производящим дознание, или по их поручению либо мотивированному ходатайству сотрудниками органа дознания.

Предложенные алгоритмы по производству указанных следственных действий как в первом, так и во втором случае направлены в первую очередь на достижение промежуточной цели расследования – получение доказательственной информации о незаконном изготовлении и распространении контрафактного программного продукта как непосредственно из показаний самого подозреваемого, так и при проведении поисковых действий на материальных объектах, которые он использует в своей повседневной деятельности.

При расследовании преступления рассматриваемого вида необходимо учитывать некоторые особенности производства обыска.

В ходе *обыска* следует осуществлять поиск машинных носителей информации, на которых сохранились следы, свидетельствующие о противоправных действиях подозреваемого с контрафактным программным продуктом. При этом особое внимание должно быть уделено изъятию средств компьютерной техники (как по месту работы, так и в жилище подозреваемого), машинных носителей информации и последующему их осмотру. Наиболее распространенным способом изготовления контрафактной программной продукции «1С: Предприятие» является замена драйверов защиты подлинной программы производителя, поэтому в ходе дальнейшего осмотра изъятых машинных носителей информации необходимо обращать внимание на ту имеющуюся компьютерную ин-

формацию, которая свидетельствует о действиях подозреваемого по изменению подлинной программы.

Если же есть основания полагать, что подозреваемый не обладал специальными знаниями по модификации драйверов защиты подлинной программы, то следует уделить внимание его электронной переписке, в процессе изучения которой может быть установлено лицо, которое произвело эти действия и предоставило контрафактную программу за вознаграждение. Не следует также исключать ситуацию, что подозреваемый действовал в составе группы и занимался только незаконным распространением контрафактного программного продукта. Также нередко контрафактный программный продукт приобретается распространителем в сети Интернет, поэтому в процессе осмотра средств компьютерной техники также должно быть исследовано и данное обстоятельство.

Если ранее полученные доказательства по уголовному делу достоверно свидетельствуют, что с лицом, у которого производится обыск, осуществлялись расчеты за установку контрафактного программного продукта, то поисковые действия должны быть направлены на отыскание заключенных договоров об оказании такой услуги и финансовых документов.

Получение доказательственной информации в ходе *допроса подозреваемого* обусловлено обстоятельствами складывающейся ситуации, которая может быть конфликтной и бесконфликтной. Следовательно, на момент принятия решения о наделении лица статусом подозреваемого и организации его последующего допроса в этом качестве следует располагать доказательственной информацией о совершенном преступлении (преступной деятельности), что позволит оперировать ею при возникновении целенаправленной конфликтной ситуации в условиях противодействия расследованию.

Принимая во внимание требования ч. 2 ст. 91 УПК о праве подозреваемого давать показания по поводу имеющегося против него подозрения, а равно по поводу иных известных ему обстоятельств, имеющих значение по уголовному делу, и имеющихся в деле доказательств, в ходе допроса подозреваемого по возможности должны быть выяснены все обстоятельства совершенного преступления:

– каков источник происхождения контрафактного программного продукта;

– каким образом была осуществлена модификация программного продукта, если она производилась подозреваемым лично;

– обладал ли подозреваемый необходимыми специальными знаниями или навыками модификации программного продукта.

Информация о возможностях модификации программного продукта правообладателя должна быть получена следователем непосредственно

до проведения следственного действия, а именно в ходе изучения личности подозреваемого в процессе подготовки к допросу.

В случае получения от допрашиваемого показаний о приобретении контрафактного программного продукта необходимо выяснить, каким образом распространенный программный продукт был приобретен и у кого. Не следует исключать случаи его приобретения подозреваемым помимо сети Интернет и в розничной торговой сети (рынки, отдельные частные торговые предприятия).

При установлении факта, что подозреваемый действовал в группе лиц по предварительному сговору, следователь обязан выяснить роль каждого соучастника. Если допрашиваемое лицо занималось только незаконным распространением контрафактного программного продукта, следует выяснить:

– как контрафактный программный продукт передавался соучастником (соучастниками) для распространения и каким образом был получен;

– каким образом распространялась информация о возможности приобретения контрафактного программного продукта непосредственно у допрашиваемого лица (объявления в средствах массовой информации, сети Интернет, через знакомых);

– кто из сотрудников организации договаривался о приобретении контрафактного программного продукта;

– каков был механизм самой процедуры;

– когда был заключен договор об установке контрафактной программной продукции;

– в какое время и на машинных носителях информации каких организаций установлен контрафактный программный продукт;

– каким образом осуществлялся расчет за установленный контрафактный программный продукт.

Устанавливая уголовную ответственность за незаконное распространение контрафактного программного продукта, в ч. 2 и 3 ст. 201 УК законодатель выделяет такие квалифицирующие признаки, как действия, сопряженные с получением дохода в крупном размере, и действия, повлекшие причинение ущерба в крупном размере. В зависимости от совершенных преступных действий следователь обязан доказать упомянутые признаки и осуществить расчет дохода или ущерба по правилам, отмеченным законодателем в примечании к ст. 201 УК.

При наличии достаточных доказательств, дающих основания для *предъявления обвинения в совершении преступления*, предусмотренного ст. 201 УК, следователь выносит мотивированное постановление о привлечении лица в качестве обвиняемого, предъявляет обвинение и допрашивает в соответствии с правилами, закрепленными в гл. 27 УПК.

Независимо от вида совершенного преступления уголовно-процессуальный закон устанавливает единую процессуальную форму для привлечения лица в качестве обвиняемого, предъявления обвинения, допроса обвиняемого. Вместе с тем обстоятельства совершенного преступления с учетом особенностей его квалификации в полной мере должны найти отражение в постановлении о привлечении лица в качестве обвиняемого, поэтому следователь, формулируя обвинение в совершении преступления, предусмотренного ст. 201 УК, обязан учитывать как положения отмеченной нормы уголовного закона, так и требования ст. 6, 15, 16, 21, 25, п. 5 ст. 39 Закона Республики Беларусь от 17 мая 2011 г. № 262-З «Об авторском праве и смежных правах».

Если подозреваемый совершил незаконное распространение контрафактного программного продукта и его действия квалифицируются по ч. 2 ст. 201 УК, то в постановлении должен быть отражен факт привлечения к административной ответственности за такое же нарушение в течение года, а в материалах уголовного дела должна находиться копия постановления суда о привлечении лица к административной ответственности за совершение административного правонарушения, предусмотренного ст. 9.21 Кодекса Республики Беларусь об административных правонарушениях за нарушение авторского права, смежных прав и права промышленной собственности.

Если же действия лица были сопряжены с получением дохода в крупном размере, то в обвинении должен найти отражение механизм их совершения (в чем они выразились) и размер дохода.

Если действия лица квалифицируются по ч. 3 ст. 201 УК, то следователь обязан отразить в постановлении, в соответствии с какими признаками нормы они были совершены: повторно, группой лиц по предварительному сговору, должностным лицом с использованием своих служебных полномочий либо эти действия причинили ущерб в крупном размере.

Таким образом, реализуя требования ст. 201 УК и ст. 241 УПК, в постановлении о привлечении лица в качестве обвиняемого следователь обязан указать:

– какую контрафактную компьютерную программу обвиняемый распространил;

– когда и на машинных носителях информации каких организаций ее установил;

– какие квалифицирующие признаки отмеченной уголовно-правовой нормы усматриваются в его преступных действиях.

В описательно-мотивировочной части обвинения, вменяя лицу каждый преступный эпизод, следователь обязан раскрыть признак контра-

фактности программного продукта, который должен не только констатироваться в постановлении о привлечении в качестве обвиняемого, но и характеризовать действия обвиняемого, связанные с модификацией программного продукта. Отмеченное обстоятельство устанавливается в процессе расследования не только в ходе осмотра программного продукта на средствах компьютерной техники, но и экспертным путем. Практика расследования по делам рассматриваемой категории свидетельствует, что следователи, констатируя признак контрафактности программы, делают ссылки на заключения эксперта и тем самым приводят в постановлении источник доказательств.

Для предварительного следствия по уголовным делам рассматриваемой категории характерна проблема вещественных доказательств. Так, при организации расследования по преступлениям против интеллектуальной собственности, когда объектом преступного посягательства является программный продукт, возникает вопрос относительно хранения и передачи в суд контрафактного программного продукта. Если в ходе расследования изымается накопитель на жестких магнитных дисках с инсталлированной контрафактной программой, то он передается вместе с материалами уголовного дела. В случае изъятия копии последней приходится иметь дело с большими объемами электронной информации и, как свидетельствует следственная практика, ее приходится хранить до решения суда на служебных компьютерах следователей, в связи с чем возникает вопрос относительно сроков ее хранения, так как уголовное дело может рассматриваться во всех судебных инстанциях. Наряду с отмеченным организационным аспектом следует констатировать, что законодатель на настоящий момент не прояснил вопрос относительно электронной информации как вещественного доказательства в действующих нормах УПК и не определил порядок изъятия, учета, хранения и передачи ее в ведомственных нормативных актах.

Таким образом, в ходе расследования по уголовному делу о преступлении против интеллектуальной собственности, когда объектом преступного посягательства является программный продукт, следователь сталкивается с отдельными обстоятельствами, характеризующими процесс производства, связанными с особенностями выемки накопителя на жестких магнитных дисках, на котором установлен контрафактный программный продукт, и его осмотром, назначением компьютерно-технической экспертизы, допросами работников организации, где выявлены факты установки контрафактного программного продукта, особенностями допроса подозреваемого и производства обыска и формулирования обвинения.

Поводами к возбуждению уголовных дел о преступлениях против интеллектуальной собственности, когда объектом преступного посягательства выступает программный продукт, являются сообщения компаний – правообладателей программной продукции и их представительств или непосредственное выявление оперативными подразделениями МВД Республики Беларусь; при принятии решения о возбуждении уголовного дела необходимо учитывать особенности конструкции ст. 201 УК.

При организации расследования ключевыми следственными и иными процессуальными действиями, позволяющими доказать виновность обвиняемого, являются:

– выемка накопителя на жестких магнитных дисках, на котором установлен контрафактный программный продукт в конкретной организации;

– осмотр изъятого накопителя на жестких магнитных дисках или копии информации с него;

– истребование документов, подтверждающих факт правообладания лицензионным компьютерным программным продуктом;

– истребование у правообладателя документов, подтверждающих стоимость лицензионной компьютерной программы;

– назначение компьютерно-технической экспертизы изъятого накопителя на жестких магнитных дисках;

– допрос работника организации, заключавшего договор на приобретение и установку компьютерного программного продукта;

– допросы работников организации, на служебных компьютерах которых установлен контрафактный программный продукт;

– выемка договора и финансовых документов, удостоверяющих оплату приобретения контрафактного программного продукта и его установку;

– задержание и допрос подозреваемого; обыск по месту жительства и работы подозреваемого;

– расчет объема ущерба с учетом количества доказанных эпизодов преступной деятельности;

– привлечение в качестве обвиняемого, предъявление обвинения и допрос обвиняемого.

5. ОРГАНИЗАЦИЯ РАССЛЕДОВАНИЯ ХИЩЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ ПЛАТЕЖНЫХ КАРТОЧЕК

В последнее время большое количество граждан Республики Беларусь обращаются в правоохранительные органы с заявлениями о хищениях денежных средств со счетов, к которым выпущены банковские платежные карточки.

Новые технологии, с одной стороны, предоставляют законопослушным гражданам новые возможности, с другой – неизбежно ведут к увеличению количества преступных посягательств в информационной среде, порождают новые виды преступной деятельности.

Скорость и масштаб развития такого инструмента, как банковские платежные карточки, хорошо иллюстрируются историей его развития.

Началом этой сферы можно считать выпуск первой кредитной карточки частной американской фирмой Smart end Roebuck. Клиенты этой компании получали на руки кусок металлической пластинки с персональными данными и подписью в начале 1920-х гг. Американские нефтяные компании вместе с крупными торговыми концернами начали выпуск карточек для постоянных и надежных клиентов для покупки за безналичный расчет товаров и услуг, предлагаемых этими фирмами.

Первая банковская кредитная карточка была выпущена в нью-йоркском районе Бруклин Дж.С. Биггинсом, специалистом по потребительскому кредиту из Национального банка «Флэтбуш». В 1946 г. Биггинс организовал работу по кредитной схеме под названием Charge-it. От клиентов местными магазинами за мелкие покупки принимались расписки, после покупки магазин сдавал расписки в банк, а банк оплачивал их со счетов покупателей. Впервые была опробована классическая цепочка расчетов, используемая в банковском карточном бизнесе по сей день.

1 октября 1958 г. была выпущена первая карта American Express. В 50-х гг. свыше 100 американских банков начали свои программы кредитных карточек. После того как в 1958 г. в карточный бизнес вступили

первый и второй по величине американские банки – Bank of America и Chase Manhattan Bank, – начался новый этап в его развитии.

С развитием новой сферы услуг банки столкнулись с препятствием, не позволявшим укрупнять свою сеть обслуживания, – местечковость карточных программ. И тогда в 1966 г. Bank of America начал выдавать лицензии на выпуск карточек BankAmericard другим банкам. В ответ на это несколько крупных банков – конкурентов Bank of America создали свою Межбанковскую карточную ассоциацию (Interbank Card Association). В июле 1970 г. была создана National BankAmericard Inc. Именно они стали принципиальными соперниками на рынке универсальных банковских карточек. Среди небанковских универсальных карточек выделялась American Express.

Параллельно с развитием рынка в США происходил процесс интернационализации операций с использованием карточек. Примерно в это же время Британская ассоциация отелей и ресторанов начала выпускать кредитную карточку BHR, которая, не являясь банковской, была все же универсальной карточкой. В 1965 г. эта система, объединившись со своим шведским конкурентом Rikskort, учредила компанию Eurocard International со штаб-квартирой в Швеции. В результате договоренностей, достигнутых в 1974 г. между американской ассоциацией Interbank Card Association и британской компанией Eurocard International, началось сотрудничество.

В 1976 г. National BankAmericard Inc. переименовала свою карточку BankAmericard в известную теперь всем Visa, а в 1980 г. Interbank Card Association дала своей карточке название MasterCard.

Конкурентная борьба между платежными системами разворачивалась и в Азии. В Японии, например, несмотря на активные попытки завоевания этого рынка Visa и MasterCard, они проигрывали пластиковым карточкам JCB. Общее количество держателей этих карточек в 1980 г. было почти в два раза больше, чем выпущенных в Японии Visa и MasterCard вместе взятых.

В настоящее время существуют несколько международных банковских ассоциаций, карточки которых популярны и обслуживаются практически во всех уголках мира, – Visa International, MasterCard International, Europay International, JCB и Diners Club.

Банки нашей страны стали осуществлять операции с использованием карточек международных банковских ассоциаций начиная со второй половины 1993 г. В марте 1994 г. ведущие белорусские банки совместно с Национальным банком Республики Беларусь приступили к созданию национальной системы безналичных расчетов на основе банковских платежных карточек «Белкарт».

Первое разрешение на право осуществления операций с использованием банковских платежных карточек Europay, MasterCard получил Белвнешэкономбанк 8 декабря 1995 г., а с карточками системы «Белкарт» – Беларусбанк 16 января 1996 г.

Для правильной квалификации хищений денежных средств из банкоматов при помощи банковских платежных карточек необходимо иметь четкое представление о способах совершения данного преступления, для чего следует уяснить основные понятия и порядок совершения операций с банковскими платежными карточками, который частично описан в Инструкции о порядке совершения операций с банковскими платежными карточками, утвержденной постановлением Правления Национального банка Республики Беларусь от 18 января 2013 г. № 34. Согласно названной Инструкции:

– авторизация – разрешение банка-эмитента и (или) владельца платежной системы на совершение операции при использовании карточки. В результате проведения авторизации возникает обязательство банка-эмитента или банка-эквайера по переводу денежных средств. Авторизация может не осуществляться в случаях, предусмотренных правилами платежной системы;

– банковская платежная карточка (далее – карточка) – платежный инструмент, обеспечивающий доступ к банковскому счету, счетам по учету вкладов (депозитов), кредитов физического или юридического лица для получения наличных денежных средств и осуществления расчетов в безналичной форме, а также обеспечивающий проведение иных операций в соответствии с законодательством Республики Беларусь (ст. 273 Банковского кодекса Республики Беларусь);

– банкомат – программно-технический комплекс, взаимодействие держателя карточки с которым осуществляется в режиме самообслуживания, обеспечивающий выдачу и (или) прием наличных денежных средств, совершение других операций при использовании карточки, регистрацию таких операций с последующим формированием карт-чека;

– банк-эквайер – банк, юридическое лицо – нерезидент, иностранная организация, не являющаяся юридическим лицом по иностранному праву, заключившие с организациями торговли (сервиса) договоры по приему и обработке информации о платежах, совершенных держателями карточек при использовании карточек, осуществлению расчетов по указанным платежам в соответствии с заключенными договорами и обслуживающие держателей карточек по операциям при использовании карточек;

– банк-эмитент – банк, банк-нерезидент, осуществляющие эмиссию карточек и принявшие на себя обязательства по перечислению денежных средств со счетов клиентов в соответствии с условиями договоров

об использовании карточек и (или) обязательства по перечислению денежных средств в соответствии с условиями кредитных договоров, предусматривающих предоставление кредита при использовании кредитной карточки;

– владелец платежной системы – юридическое лицо либо иностранная организация, не являющаяся юридическим лицом по иностранному праву, определяющие правила платежной системы и исполняющие обязательства в соответствии с правилами и заключенными с участниками платежной системы договорами;

– компрометация карточки – наличие у любого лица, не являющегося законным держателем карточки (за исключением банка-эмитента, процессингового центра), сведений о реквизитах действительной карточки и (или) иной информации, позволяющей несанкционированное использование действительной карточки;

– мошеннические действия держателя карточки – действия держателя карточки, совершаемые с целью обмана участников платежной системы путем имитации хищения карточки или несанкционированного использования карточки либо ее реквизитов;

– платежный терминал самообслуживания – программно-технический комплекс, устанавливаемый в организации торговли (сервиса) в соответствии с договором эквайринга и предназначенный для регистрации совершаемых при использовании карточки в режиме самообслуживания операций оплаты непосредственно реализуемых организацией торговли (сервиса) товаров (работ, услуг) или иных платежей, совершаемых в соответствии с законодательством, и получения установленных банком информационных и иных услуг с последующим формированием карт-чека;

– процессинг – деятельность по сбору и обработке информации, поступающей от организаций торговли (сервиса), банкоматов, инфокиосков, пунктов выдачи наличных денежных средств либо из иных источников в зависимости от технологий, используемых участниками платежной системы, а также по передаче обработанной информации для осуществления безналичных расчетов;

– процессинговый центр – банк либо иное юридическое лицо, иностранная организация, не являющаяся юридическим лицом по иностранному праву, осуществляющие процессинг на основании договоров с иными участниками платежной системы, заключенных в соответствии с правилами платежной системы;

– реквизиты карточки – номер, срок действия карточки и иная информация в соответствии с правилами платежной системы (банка-эмитента).

Правила осуществления операций с использованием карточек определяются владельцем конкретной системы расчетов. Банки Республики Беларусь сегодня являются участниками трех международных систем

(Visa International, MasterCard International и JCB) и одной внутренней системы («Белкарт»).

Visa International в настоящее время является крупнейшей в мире платежной организацией и занимает порядка 60 % рынка банковских карт.

Вопреки широко распространенному мнению ассоциация Visa – это не компания по выпуску карточек, а электронная расчетная система, предшественницей которой действительно была компания по выпуску кредитных карточек.

Ассоциация Visa – транснациональная корпорация, в которой контрольный пакет не принадлежит никому. Это ассоциация, находящаяся в совместной собственности более 20 тыс. финансовых учреждений, расположенных по всему миру. Сама ассоциация Visa непосредственно не обслуживает клиентов или торговые точки. Через своих членов ассоциация Visa обеспечивает функционирование всемирной сети перемещения средств. Она обеспечивает служебную электросвязь во всемирном масштабе, устанавливает технические нормативы и разрабатывает новые виды услуг, тем самым давая своим членам – финансовым организациям возможность обеспечить как их клиентам – держателям карточек, так и торговым точкам удобное и недорогое средство совершения большого числа разнообразных сделок во всем мире.

Ассоциация Visa разделена на шесть географических регионов: Азиатско-Тихоокеанский регион; Канада; Центральная Европа, Ближний Восток и Африка (CEMEA); Европейский союз; Латинская Америка; Соединенные Штаты Америки.

Платежная система состоит из трех отдельных элементов – собственно ассоциации, банка-эмитента (банка, который выдает карточки) и банка-эквайера (банка, который работает с торговыми точками). Хотя членами ассоциации являются как банки-эмитенты, так и банки-эквайеры, каждый банк-эмитент и банк-эквайер являются самостоятельными предприятиями.

Обработка карточек представляет собой систему взаимосвязи, конечными элементами которой являются банки, а платежная система – посредником. Один и тот же банк может служить как банком-эмитентом, так и банком-эквайером. Получив заявление от какого-либо частного лица или компании, банк-эмитент карточки изучает кредитную историю заявителя и в случае положительного решения выдает карточку. Карточки выдаются на конкретных условиях, которые могут предусматривать годовую комиссию и взимание процентов, если весь остаток не оплачивается в течение конкретно оговоренного срока, обычно в течение 20 дней с даты выставления счета.

По кредитным карточкам устанавливается также кредитный лимит в диапазоне от нескольких сотен до многих тысяч долларов.

Банк-эквайер организует принятие торговыми точками оплаты с помощью карточек и взимает за эту услугу комиссию, обычно в виде определенной процентной доли. Каждый банк сам устанавливает комиссию, взимаемую с той или иной торговой точки. Сюда входят услуги по проведению авторизации и расчетов. В случае если торговая точка и держатель карточки используют один и тот же банк и (или) один и тот же расчетный центр, то некоторые этапы оформления оказываются ненужными и издержки банка уменьшаются. Наиболее значительные затраты при этом приходятся на межбанковскую комиссию за операции с карточками других банков-эмитентов.

Когда держатель карточки использует свою карточку для оплаты товаров или услуг, работник торговой точки проводит карточку через электронный POS-терминал (от англ. point of sale – точка оплаты) – устройство для приема карточек к оплате. После этого работник просит покупателя подписать распечатку с электронного POS-терминала или платежную квитанцию и убеждается в действительности карточки. Покупатель получает один экземпляр квитанции, в то время как торговая точка оставляет один экземпляр себе. Затем банк-эквайер передает информацию о покупке (либо введенные данные о покупке, либо информацию, считанную электронным образом) в платежную систему. Затем платежная система подтверждает, что номер счета является законным и не блокирован. Также данная информация, равно как и номер счета, сумма сделки и дата истечения срока действия карточки, затем препровождается банку, выдавшему карточку. Эта информация может быть проверена и сверена с контрольной величиной (CVV – для Visa, CVS – для MasterCard) и затем возвращается в торговую точку. Указанный процесс, в ходе которого информация о продажах собирается, сортируется и препровождается банку-эмитенту платежной системой, называется клирингом.

Для организации расследования уголовных дел данной категории необходимо хорошо понимать механизм совершения преступления. Так, часто совершение рассматриваемых преступных деяний начинается с изготовления или приобретения так называемого скиммера – устройства, предназначенного для несанкционированного копирования сведений с магнитной полосы карточек. Оно скрытно устанавливается на картоприемник банкомата. Скиммеры оборудованы магнитной головкой для считывания сведений с магнитной полосы, элементами питания и энергонезависимой памятью, которая дает возможность сохранять сведения после разрядки батареек. Более современные скиммеры оборудованы радиоэлементами, позволяющими передавать полученные данные на расстоянии посредством GSM-, Bluetooth- или ИК-связи (например, в виде СМС).

Сведения, находящиеся на магнитной полосе карточки, называются дампом и представляют собой набор цифр и других символов, разделенных знаком равенства. Дампы можно обнаружить в ходе осмотра средств компьютерной техники, изъятых у подозреваемых.

Дамп (как полный, так и сокращенный) может быть записан на магнитную полосу другой пластиковой карточки. Таким образом будет создан дубликат карточки, пригодный для использования в банкомате при условии введения правильного ПИН-кода.

Для получения сведений о ПИН-коде также используются специальные устройства. Обычно это накладка на клавиатуру банкомата, так называемый пинпад. Он повторяет оригинальную клавиатуру банкомата и устанавливается на нее посредством двустороннего скотча. Для того чтобы клавиатура не выступала над поверхностью банкомата, может использоваться фальшивая панель, покрывающая всю соответствующую поверхность банкомата. Реже для получения сведений о ПИН-коде используется миниатюрная видеокамера, которая устанавливается в месте, с которого хорошо фиксируются нажатые клавиши.

В подавляющем большинстве случаев скиммеры и пинпады преступники приобретают через сеть Интернет у лиц, специализирующихся на их изготовлении. Данные устройства приобретаются в комплекте (скиммер и пинпад). Оплата осуществляется электронными деньгами или посредством международных денежных переводов. Способы доставки согласовываются индивидуально.

Обычно скиммер и пинпад устанавливают на банкоматы в центральной части города, где ими пользуются более оживленно и более имущие граждане. Самые популярные места – около гостиниц, с расчетом на иностранцев.

Банкомат воспринимает карточку только по магнитной полосе, поэтому ее внешний вид значения не имеет. Исключением являются более современные чиповые карточки, или так называемые гибридные, которые кроме магнитной полосы имеют микрочип. Однако многие банкоматы до сих пор не переоборудованы соответствующим устройством и по-прежнему воспринимают эти карточки только по магнитной полосе. В таком случае, по правилам международных платежных систем, все затраты в результате хищения возлагаются на банк, который не оборудовал свой банкомат устройством для работы с чиповыми карточками.

В качестве заготовок, на которые преступники записывают дамп, могут использоваться:

– подлинные карточки с истекшим сроком действия, найденные или похищенные карточки;

– дисконтные карточки с магнитной полосой;

– телефонные и иные карточки с магнитной полосой;

– чистые пластиковые карточки с магнитной полосой, которые находятся в свободной продаже для легального изготовления дисконтных карточек (обычно имеют чистую поверхность белого, серебристого или золотистого цвета – отсюда пошло название «белый пластик», которым обозначаются преступления данного вида независимо от фактического цвета поддельных карточек).

Запись дампов на заготовки производится с помощью компьютера и специального устройства, которое называется картридером (программатором, энкодером).

Картридеры бывают различных моделей и также находятся в свободной продаже. Эти устройства производятся серийно, и по наименованию модели можно получить сведения об их назначении и технических характеристиках.

При изготовлении поддельных карточек соответствующие им ПИН-коды обычно наносят либо непосредственно на карточку, либо на отдельную бумагу. В таких случаях поддельные карточки нумеруют, чтобы преступник мог ориентироваться, какому порядковому номеру соответствует ПИН-код. Данное обстоятельство можно использовать в доказательственных целях – минимальное количество поддельных карточек может быть установлено по наибольшему порядковому номеру из числа изъятых карточек.

Хищения совершаются путем помещения поддельной карточки в банкомат, введения ПИН-кода и запрашиваемой суммы денежных средств. Часто при использовании в Беларуси иностранных карточек посмотреть остаток средств на карт-счете бывает невозможно. Тогда в распечатке операций по карточке можно наблюдать так называемую лесенку. Преступник запрашивает крупную сумму, например 500 р., получив отказ, запрашивает 300 р., затем 200 р., 100 р. и т. д., пока не получит деньги. Или в обратном порядке: получив 10 р., запрашивает 20 р., затем 50 р. и т. д. Это обстоятельство указывает на то, что человек не владеет сведениями о доступном остатке средств на счете, и может использоваться в ходе допросов.

Нередко перед совершением хищений преступник заклеивает глазок встроенной в банкомат видеокамеры (наклейкой, жвачкой и т. д.). В таких случаях целесообразно провести осмотр места происшествия на предмет установления других возможных средств видеонаблюдения, поскольку банкоматы часто располагаются в торговых точках, рядом с учреждениями и в других местах, где, возможно, установлены технические средства, имеющие функцию фотосъемки или видеозаписи.

Если преступник использует скиммер, то он получает реквизиты сразу десятков и сотен карточек. Однако использовать их все для со-

вершения хищений довольно сложно. Это вызвано тем, что, как только начнутся хищения и люди, у которых пропали деньги, обратятся в банк, служба безопасности выявит, когда и на каком банкомате был установлен скиммер (где заявители использовали свои карточки в одно и то же время). Это так называемая точка компрометации. Все карточки, которые использовались в этом банкомате в соответствующий период, блокируются. Обычно банки успевают среагировать в течение одной недели. Исключение – когда скиммер установлен в туристических или курортных городах, где вычислить точку компрометации сложнее.

Для обналичивания наибольшего количества карточек преступник должен действовать быстро. Съятие денег в банкомате – один из самых опасных для него этапов преступления, поскольку есть вероятность быть задержанным с поличным. В связи с этим для непосредственного совершения хищений привлекаются помощники, так называемые дропы. Они обналичивают карточки за определенный процент. Чаще всего – половина от снятого.

Уголовные дела данной категории, как и все остальные, могут быть возбуждены как по факту (по заявлению банка или гражданина), так и в отношении лица, задержанного с поличным либо установленного в ходе доследственной проверки. Последний вариант наиболее предпочтителен, поскольку позволяет подготовиться к реализации оперативных материалов, собрать первоначальную доказательственную базу, спланировать одновременные обыски и задержания всех подозреваемых.

Основой расследования уголовных дел данной категории является систематизация всех сведений о совершенных хищениях в единую таблицу. Такая таблица при правильной организации будет являться планом расследования, поскольку в ней можно отражать, что не сделано по каждому конкретному эпизоду, источником доказательств, основой будущего обвинения и справки о доказанности. Для составления таблицы наиболее удобно использовать программу Microsoft Excel.

На *начальном этапе расследования* необходимо в первую очередь проанализировать все имеющиеся сведения об операциях, совершенных посредством поддельных карточек, и систематизировать их в хронологическом порядке согласно следующим реквизитам:

– дата хищения;

– время или период хищения (совершения ряда последовательных операций посредством одной и той же карточки в одном и том же банкомате);

– номер, содержащийся на магнитной полосе поддельной карточки;

– похищенная сумма;

– сумма покушения;

– эквивалент суммы в белорусских рублях на день хищения;

– причина отказа в выдаче денег при покушении;

– адрес банкомата, из которого совершено хищение (покушение);

– банк-эквайер (владелец банкомата);

– банк-эмитент (выпустивший подлинную карточку с таким номером);

– держатель карточки (если установлен).

Эта часть таблицы после заполнения составит основу постановления о привлечении в качестве обвиняемого, поскольку каждая строка таблицы будет соответствовать отдельному эпизоду хищения.

Конвертировать таблицу в готовое обвинение (за исключением описательной части) можно в автоматическом режиме посредством функционала программ Microsoft Excel и Microsoft Word.

При установлении подозреваемого таблицу желательно дополнить реквизитами, отражающими имеющиеся доказательства по каждому эпизоду:

– наличие фото- или видеоматериалов с технических средств, имеющих функцию фотосъемки или видеозаписи, совершения конкретного эпизода хищения с пометкой о том, кто на ней изображен;

– кто из обвиняемых находился в момент хищения (или непосредственно до либо после его совершения) в той же соте, что и соответствующий банкомат;

– какие пометки содержатся на поверхности поддельных карточек, изъятых банкоматами или у подозреваемых;

– сведения о заявленных исках, другие сведения, представляющие интерес по уголовному делу;

– сведения, связанные с планированием расследования (допрошен ли держатель карточки, направлены ли соответствующие запросы).

Кроме того, доказательством будут являться и сами факты совершения хищений в их соотношении (пересечении) друг с другом.

Название банка и государство, в котором выпущена карточка, можно установить по первым шести цифрам ее номера. Это так называемый БИН (банковский идентификационный номер). Сведения о принадлежности БИН конкретным банкам можно запросить в банках Республики Беларусь либо оперативно получить указанную информацию на соответствующих ресурсах сети Интернет, например http://www.binbase.com/search.html или https://www.bindb.com/bin-database.html.

Если в результате анализа указанной информации или дальнейшего расследования будут установлены сведения о других карточках, которые могли быть использованы преступниками, нужно запросить в банках Беларуси сведения о всех операциях по каждой из таких карточек. При этом выносится постановление о получении сведений, составляющих банковскую тайну (согласно ч. 3 и 8 ст. 36, ст. 100, 103 УПК, ст. 121 Банковского кодекса Республики Беларусь), которое санкционируется прокурором.

Поскольку переписка с банками и процессинговыми центрами занимает длительное время, в постановлении целесообразно поставить сразу все интересующие вопросы. Например, можно *запросить сведения*:

– о транзакциях, совершенных в устройствах банков с использованием перечисленных карточек в определенный период (в том числе об отклоненных транзакциях);

– транзакциях, зарегистрированных соответствующими банкоматами за 15 минут до и 15 минут после каждой транзакции с перечисленными карточками;

– банках-эмитентах перечисленных карточек, а также иных иностранных карточек, которые использовались в указанные периоды времени;

– наличии фото- или видеоматериалов с технических средств, имеющих функцию фотосъемки или видеозаписи, или осуществленных устройствами банкоматов при использовании перечисленных карточек;

– фактах изъятия устройствами банков каких-либо из перечисленных карточек и местах их хранения (такие карточки необходимо подготовить для производства выемки);

– оспорены ли банками-эмитентами транзакции, совершенные посредством перечисленных карточек. Если да, то кому причинен материальный ущерб и на какую сумму? Если нет, то необходимо связаться с банками-эмитентами по имеющимся каналам и выяснить, признаны ли такие транзакции противоправными (мошенническими).

После анализа полученного ответа могут быть установлены новые номера карточек, предположительно являющихся поддельными, что влечет необходимость направления новых запросов.

Кроме того, в *первоочередном порядке* необходимо выполнить следующие действия.

1. Направить в те государства, где находятся банки-эмитенты, поручения или просьбы об оказании правовой помощи в проведении в банках выемки сведений о держателях карточек, их заявлений о несанкционированных операциях по счетам с выпиской детализированных сведений по таким операциям, о том, возмещены ли держателям соответствующие суммы и кто понес ущерб в результате хищений, а также в проведении допросов держателей по аналогичным вопросам. Для ускорения исполнения просьбы и поручения целесообразно продублировать по каналам Интерпола.

При наличии достаточных доказательств уголовное дело может быть передано прокурору для направления в суд до получения материалов исполненных просьб и ответов из национальных центральных бюро Интерпола, поскольку, как показывает практика, такие ответы могут поступать через несколько лет после направления запросов или не поступать вовсе.

2. Произвести в соответствующих банках выемку и осмотр фото- или видеоматериалов с устройств, имеющих функцию фотосъемки или видеозаписи, или осуществленных устройствами банкоматов при совершении хищений (покушений). Изымать желательно сразу на компакт-дисках (в распечатанном виде хуже качество изображения, а информацию с флэш-карты в любом случае придется перезаписывать на компакт-диск при окончании расследования). Видеозаписи обычно хранятся до трех месяцев, поскольку при исчерпании свободного места на накопителе новая информация пишется поверх старой (так называемая циклическая запись). Промедление в данном случае может повлечь утрату важнейшего доказательства.

3. Произвести осмотр места происшествия на предмет установления иных источников видеонаблюдения за банкоматом.

4. Произвести в соответствующих банках выемку и осмотр поддельных карточек, изъятых банкоматами при совершении покушений на хищения. После выемки в отношении таких карточек желательно назначить дактилоскопическую и генетическую экспертизы (при условии осторожного обращения с ними со стороны работников банков, в том числе при извлечении из карт-приемников банкоматов). Впоследствии данные карточки необходимо осмотреть с использованием картридера (устройства для чтения сведений с магнитной полосы карточки), при отсутствии которого можно обратиться в банк и произвести осмотр с участием специалиста и задействованием имеющихся там устройств, либо назначить экспертизу карточек по следующим вопросам:

– какая информация содержится на магнитных полосах пластиковых карточек, представленных на исследование; соответствует ли ее содержание требованиям, предъявляемым платежными системами;

– возможно ли использовать представленные пластиковые карточки как средства получения наличных денежных средств, оплаты товаров, услуг?

5. Если изъят скиммер или пинпад, в отношении их назначается экспертиза радиоэлектронных устройств по следующим вопросам:

– чем являются представленные на исследование устройства;

– являются ли представленные на исследование устройства орудием для получения сведений о реквизитах карточек (сведений с магнитной полосы и ПИН-кода);

– составляют ли представленные на исследование устройства полный комплект, позволяющий использовать его по целевому назначению;

– находится ли данное устройство (устройства) на момент исследования в работоспособном состоянии; если да, то каковы его основные технические характеристики;

– промышленным или самодельным способом изготовлено данное устройство (устройства);

– способно ли данное устройство (устройства) направлять какие-либо сведения посредством Bluetooth-, ИК- или GSM-связи; если да, то на какой абонентский номер (номера);

– имеются ли признаки, позволяющие сделать вывод об успешном использовании указанного устройства по целевому назначению; если да, то какие?

6. Направить в соответствующие банки-эквайеры письма с разъяснением права на заявление гражданских исков по делу. Банкам разъясняется право на заявление гражданского иска даже в том случае, когда известно, что операции, которые установлены как хищения, банком-эмитентом не оспорены. Иностранный банк, понесший убытки в результате хищения, не всегда оспаривает такие операции у белорусских банков, поскольку избегает урона для своей деловой репутации или получил возмещение ущерба в страховых организациях. В результате в уголовном процессе складывается коллизия, при которой не установлен субъект, понесший ущерб в результате хищения. Согласно сложившейся практике такие эпизоды хищений также вменяются в вину обвиняемым при наличии достаточных доказательств их совершения конкретными обвиняемыми. При этом следует учитывать, что непосредственное изъятие денег всегда осуществляется у банка-эквайера из принадлежащего ему банкомата. А все последующие взаиморасчеты между банками относятся к категории гражданско-правовых отношений.

7. При производстве задержаний и обысков необходимо обратить особое внимание на обнаружение и изъятие:

– поддельных карточек, а также карточек без признаков подделки, так как на магнитной полосе могут быть записаны реквизиты другой карточки;

– соответствующих по цвету маркеров, фломастеров и других пишущих принадлежностей для последующего назначения химической экспертизы, если поддельные карточки содержат на поверхности рукописные пометки;

– одежды подозреваемых, в которой они запечатлены на видеозаписях, в том числе головных уборов, наручных часов, браслетов, колец, перчаток и других предметов;

– носителей информации (компьютеры, накопители на жестких магнитных дисках, флэш-карты, мобильные телефоны и т. д.), в которых могут содержаться сведения о дампах и ПИН-кодах, отчеты о похищенных суммах для представления возможным соучастникам, фрагменты переписки с соучастниками посредством различных интернет-коммуникаторов или СМС, иные сведения. Изъятые носители информации впоследствии желательно осматривать с участием специалиста, поскольку интересующие сведения могут быть зашифрованы и скрыты с использованием специальных программ;

– картридеров, скиммеров и других устройств, назначение которых не установлено, для последующего проведения экспертиз;

– банковских документов.

8. Запросить уголовные дела из других следственных подразделений. Если таковые возбуждены по установленным эпизодам хищений, то соединить их. При наличии отказных материалов инициировать отмену постановлений об отказе в возбуждении уголовных дел и приобщить их к делу.

9. В ходе допросов подозреваемых и обвиняемых обратить особое внимание на происхождение у них поддельных карточек. Наиболее часто они признают снятие ими денег из банкоматов, но отрицают свою вину, поскольку якобы действовали по чьей-то просьбе (использовались в качестве дропов), были введены в заблуждение и не понимали преступного характера своих действий. При этом их показания часто противоречивы. В зависимости от следственной ситуации им можно поставить, например, такие вопросы:

– имеют ли они собственные карточки и понимали ли, что те карточки, которые они использовали, поддельные;

– почему, когда карточки изымались банкоматами, они не обращались в соответствующие банки с требованием об их возврате;

– где находятся оставшиеся карточки; если они уничтожены, то по какой причине;

– какой процент полученных денег оставляли себе и на каком основании;

– почему использовали различные банкоматы в различных точках города, а не сняли все деньги сразу со всех карточек в одном и том же банкомате;

– почему снимали деньги в вечернее и ночное время;

– почему прятали или маскировали свою внешность?

Есть некоторые отличия в расследовании уголовных дел в зависимости от того, где произошла компрометация карточек (т. е. был установлен скиммер) и где совершались хищения.

В практике более часто встречаются случаи, когда хищения совершаются в Беларуси с использованием иностранных поддельных карточек, компрометация которых произошла в государствах Евросоюза, курортных или туристических центрах. В таких случаях, несмотря на сотни

установленных эпизодов хищений, потерпевших по делу немного. Держателями карточек являются иностранцы, которых не всегда удается установить. Работать приходится только с банками, выступающими в качестве гражданских истцов.

Если скиммер был установлен в Беларуси, то расследование будет осложнено большим количеством потерпевших по делу независимо от того, где совершались хищения – в Беларуси или за рубежом. Даже если банками возмещен причиненный гражданам ущерб, держатели карточек могут быть признаны потерпевшими по делу в связи с причинением им морального вреда.

Алгоритм расследования хищений с использованием карточек выглядит следующим образом:

– осмотр места происшествия (места хищения карточки, банкомата, с использованием которого с карт-счета карточки были похищены деньги);

– допрос потерпевшего;

– допросы свидетелей;

– запрос у банка-эмитента о движении (расходно-приходным операциям) по карт-счету карточки;

– запрос у банка-эквайера об операциях, осуществленных с использованием банкомата в период совершения хищения, об оборудовании банкомата техническими средствами, имеющими функцию фотосъемки или видеозаписи, и о наличии видеозаписи периода совершения преступления;

– при наличии видеозаписи – производство ее выемки, последующий осмотр с целью установления личности злоумышленника;

– запрос у компаний мобильной связи о телефонных звонках, совершенных в соте места хищения карточки в период ее хищения и в соте нахождения банкомата в период снятия с его помощью денежных средств с карточки;

– последующий сравнительный осмотр полученных сведений для установления возможного номера мобильного телефона, которым пользовался злоумышленник;

– при установлении личности злоумышленника – производство обыска по месту его жительства для обнаружения похищенной карточки, снятых с карт-счета денежных средств или имущества, приобретенного за такие средства;

– по возможности производство дактилоскопической экспертизы карточки;

– иные следственные и процессуальные действия.

6. ОРГАНИЗАЦИЯ РАССЛЕДОВАНИЯ ИЗГОТОВЛЕНИЯ И РАСПРОСТРАНЕНИЯ ПОРНОГРАФИЧЕСКИХ МАТЕРИАЛОВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ КОМПЬЮТЕРНОЙ ТЕХНИКИ

По данным Всемирной организации труда, в порносъемках в мире ежедневно принимают участие более 3 млн человек, из них более 1 млн детей. В сети Интернет находится свыше 1 млрд страниц с порнографией, и это число постоянно растет.

Наблюдаемая в последнее время общемировая тенденция развития проблемы распространения порнографии не обошла стороной и Беларусь. При этом все же можно констатировать, что проблема распространения порнографии в сети Интернет не стала в нашей стране масштабным явлением.

Своим происхождением термин «порнография» (греч. pornē – развратник и grapho – пишу) обязан появлению в XVIII в. во Франции книги Ретиф де ла Бретонна «Порнограф, или Размышление порядочного человека об истинной безнравственности проституции», в которой рассматривались сферы жизнедеятельности человека, традиционно считавшиеся в обществе неприличными, ввиду чего слово «порнография» стало нарицательным понятием непристойности, связанной с сексуальностью.

Порнографическое представление полового акта и половых органов вопреки распространенному мнению не является изобретением современности. На фресках Древнего Рима и античных вазах можно увидеть подобные мотивы. Аналогичные изображения встречаются на керамике в Перу. Начиная с эпохи Возрождения и до XVIII в. были распространены «порнографические» гравюры. С появлением фотографии в XIX в. и кинематографии в XX в. порнографическое представление сексуальности получило новый виток развития.

Одной из самых сложных проблем, возникающих в области уголовно-правовой борьбы с порнографией, является проблема легального

определения данного понятия. Трудность заключается в том, что порнография в высокой степени культурно обусловленное явление, т. е. отнесение того или иного вида произведений к порнографическим зависит от принятых в отдельно взятом обществе морально-этических стандартов, границ допустимого. В силу указанных различий нормы международного публичного права не содержат универсального определения порнографии, оно дается в национальных законодательствах.

В тексте уголовного закона общее определение порнографии встречается весьма редко (уголовные кодексы Китая, Норвегии, Румынии, Словакии, штата Нью-Йорк).

Так, в ст. 367 УК Китая под порнографической продукцией понимаются печатные издания, фотографии, видео-, аудиокассеты, картины и иная продукция, подробно описывающие сексуальные действия или откровенно пропагандирующие секс. Научные издания по физиологии человека и медицине не являются порнографией. Произведения литературы и искусства сексуального (эротического) содержания, имеющие культурную ценность, не подпадают под определение порнографии.

В УК Норвегии (§ 204) под порнографией понимаются «сексуальные изображения, которые действуют вызывающе или иным способом умаляют ценность человека, разлагают или унижают; сексуальные изображения включают те, в которых используются дети, трупы, животные, насилие и принуждение». При этом порнографией не считаются сексуальные изображения, которые должны рассматриваться как дозволительные с художественной, научной, информационной или подобной точки зрения. Далее норвежский законодатель уточняет, что § 204 не действует в отношении фильмов или видеоматериалов, одобренных при предварительном контроле Госфильмнадзором для коммерческого показа или продажи.

Ст. 235.00 УК штата Нью-Йорк дает следующее определение термина «непристойный»[1]: любой материал или постановка «непристойны», если среднее лицо, применяя современные стандарты общества, нашло бы, что они имеют преобладающую апелляцию к похотливому интересу к сексу и изображают или описывают очевидно оскорбительным способом, фактическим или имитируемым половое сношение, содомию, скотоложство, мастурбацию, садизм, мазохизм, испражнение или непристойную демонстрацию гениталий и, рассматриваемые в целом, они

[1] Понятие «порнография» (pornography) в США в содержательном смысле ближе к нашему понятию «эротика». Такие порнографические произведения защищены первой поправкой к Конституции США, гарантирующей свободу слова и печати, т. е. их распространение может ограничиваться, но не запрещается. Термин же, используемый для произведений, содержащих элементы порнографии в нашем понимании, – «непристойный» (obscene).

лишены серьезной литературной, художественной, политической или научной ценности.

Нередко легальное определение порнографии дается вне рамок уголовного законодательства. Согласно ст. 1 закона Украины от 20 ноября 2003 г. № 1296-IV «О защите общественной морали» под порнографией понимается «вульгарно-натуралистическая, циничная, неприличная фиксация половых актов, самоцельная, специальная демонстрация гениталий, антиэтических сцен полового акта, сексуальных извращений, зарисовок с натуры, не отвечающих моральным критериям, оскорбляющих честь и достоинство человека, пробуждая недостойные инстинкты».

В уголовном законодательстве мусульманских стран (Алжир, Афганистан, Египет, Ирак, Иран) вообще не используется понятие «порнография», а говорится об изображениях и иных объектах, противных приличиям (Алжир), противоречащих культуре и общественным нравам (Афганистан), наносящих урон общественной морали и целомудрию (Иран). Очевидно, что это очень расплывчатое и широкое понятие, под которое можно подвести самые невинные, с точки зрения европейца, вещи. Например, в таких странах, как Иран, ОАЭ, Саудовская Аравия, Судан, оскорблением нравов, безусловно, являются изображение женщины в купальнике или «откровенные» сцены поцелуев в фильме.

Важное значение для трактовки понятия «порнография» («непристойность») имеет содержащаяся в уголовных законах ряда стран (Великобритания, Индия, Иран, Канада, Китай, Новая Зеландия, Норвегия, Швейцария) специальная оговорка, согласно которой к порнографии не относятся произведения, представляющие художественную или научную ценность, либо если их демонстрация (распространение) служит общественному благу. Так, согласно примечанию к ст. 640 УК Ирана ее положения не относятся к материалам, которые подготавливаются либо по ним совершается сделка для научных целей и (или) для любого другого законного и целесообразного использования, если при этом соблюдаются правила, установленные шариатом. В соответствии с п. 5 ст. 200 УК Швейцарии предметы или показы не являются порнографическими, если они имеют охраняемую культурную или научную ценность. Британский Акт о непристойных публикациях 1959 г. также исключил из порнографии все, что имеет художественную или научную ценность. Согласно этому закону лицо не может быть обвинено в преступлении, если будет доказано, что публикация рассматриваемого произведения оправдана общественным благом на том основании, что она способствует интересам науки, литературы, искусства, просвещения или иным целям, представляющим общий интерес. Сразу после принятия данного акта в 1960 г. состоялся исторический процесс над романом

Д.Г. Лоренса «Любовник леди Чаттерлей», в результате запрет на книгу был отменен[1].

В любом случае следует отметить, что поскольку критерии высокохудожественности достаточно размыты и произвольны, то по общедоступному телевидению в одних странах могут показывать фильмы, которые в других государствах признаны порнографическими.

Традиционная японская культура весьма толерантно относится к изображению полового акта и т. п. В Японии по закону разрешено рисовать и реализовывать в открытой продаже любую порнографию, в том числе с участием детей, зверей и сценами насилия, при условии, что у персонажей лица будут не человеческие, а игрушечные (отсюда столь распространенное в мире японское «анимэ»).

В белорусском законодательстве определение порнографии дано в п. 2 Инструкции о порядке выпуска, тиражирования, показа, проката, продажи и рекламирования эротической продукции, продукции, содержащей элементы эротики, насилия и жестокости, продукции по сексуальному образованию и половому воспитанию, а также продукции сексуального назначения, утвержденной постановлением Министерства культуры Республики Беларусь от 8 мая 2007 г. № 18, в соответствии с которым порнография – «вульгарно-натуралистическая, омерзительно-циничная, непристойная фиксация половых сношений, самоцельная, умышленная демонстрация большей частью обнаженных гениталий, антиэстетичных сцен полового акта, сексуальных извращений, зарисовок с натуры, которые не соответствуют нравственным критериям, оскорбляют честь и достоинство личности, ставя ее на уровень проявлений животных инстинктов».

Порнографическими считаются материалы:

– способ подачи информации которых выходит за общепринятые в настоящих культурно-исторических рамках границы откровенности;

– в основном или исключительно предназначенные для стимулирования сексуальных реакций субъектов, эту информацию воспринимающих;

– не представляющие художественной ценности[2].

Некоторые авторы предлагают также в качестве существенного признака порнографических материалов рассматривать такой критерий, как их неавторизованность, т. е. анонимность авторов, режиссеров, актеров. Полагаем, что это неверно, поскольку указание авторства на материале еще не гарантирует того, что по своему содержанию он не является порнографическим (например, в Калифорнии (США) существуют и активно действуют несколько легальных киностудий, изготавливающих исключительно порнографическую, в нашем понимании, продукцию).

[1] См. об этом: Капинус О.С., Додонов В.Н. Ответственность за порнографию в современном уголовном праве [Электронный ресурс]. URL: http://dmitrich-gth.ya.ru/replies.xml?item_no=17.

[2] См.: Бугаев К.В. Экспертное сопровождение расследования преступлений, предусмотренных ст. 242 УК РФ (Незаконное распространение порнографических материалов или предметов) // Законодательство и практика. 2010. № 1. С. 28.

Кроме того, в качестве основных признаков порнографических произведений выделяют:

– отсутствие сюжета либо его крайний примитивизм, лишь позволяющий связать между собой отдельные сцены половых актов;

– изображение крупным планом половых органов, половых актов и иных сексуальных действий;

– часто встречающаяся сопряженность событий со сценами противоестественных и противоприродных способов удовлетворения половой страсти, изображениями группового полового акта, сексуальных отношений с участием детей[1].

Проблема борьбы с распространением порнографии давно волнует мировую общественность. В отдельных государствах допускается возможность легального оборота в строго ограниченных пределах, в других – провозглашен полный запрет такого оборота под страхом уголовного наказания.

Так, в соответствии с УК Австрии наказуемы только производство и оборот детской порнографии, в Бельгии, Испании, Словении – только детской порнографии и распространение порнографии среди несовершеннолетних. В некоторых странах (Германия, Латвия, Финляндия, Чехия, Швейцария) в уголовном законодательстве вся порнографическая продукция делится на две категории: относительно допустимую (обычная порнография) и абсолютно недопустимую (квалифицированная порнография). К последней категории относятся детская порнография, а также изображение насильственных сексуальных действий и некоторых половых извращений. Например, ч. 3 ст. 198 УК Швейцарии к квалифицированной порнографии относит предметы или представления, «которые по своему содержанию включают в себя сексуальные действия с детьми или с животными, с человеческими экскрементами или насильственную деятельность», а ч. 2 ст. 166 УК Латвии – «материалы порнографического характера… в которых описаны или изображены сексуальное использование детей, сексуальные действия людей с животными, некрофилия или насилие порнографического характера».

По общей для вышеперечисленных стран схеме производство и оборот квалифицированной порнографии наказуемы всегда, тогда как распростра-

[1] См.: Научно-практический комментарий к Уголовному кодексу Республики Беларусь / Н.Ф. Ахраменка [и др.] ; под ред. А.В. Баркова, В.М. Хомича. 2-е изд., с изм. и доп. Минск : ГИУСТ БГУ, 2010. С. 794.

нение обычной порнографии преследуется лишь в специально указанных случаях (демонстрация детям или неограниченной аудитории).

В целом признавая повышенную общественную опасность указанных преступлений, международное сообщество приняло ряд нормативных правовых актов, среди которых отдельно следует выделить:

– Международную Конвенцию по пресечению обращения порнографических изданий и торговли ими (Женева, 12 сентября 1923 г., в редакции от 12 ноября 1947 г.);

– Соглашение о борьбе с распространением порнографических изданий (Париж, 4 мая 1910 г., с изменениями от 4 мая 1949 г.);

– Конвенцию о запрещении и немедленных мерах по искоренению наихудших форм детского труда (Конвенция 182) (принята на 87-й сессии Генеральной конференции Международной организации труда, Женева, 1 июня 1999 г.);

– Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии (принят резолюцией 54/263 Генеральной Ассамблеи ООН от 25 мая 2000 г.).

Отчасти реализацией положений этих актов является введение уголовной ответственности за распространение порнографических материалов в Республике Беларусь, которая предусмотрена ст. 343 «Изготовление и распространение порнографических материалов или предметов порнографического характера» и ст. 343[1] «Изготовление и распространение порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего» УК.

Уголовно наказуемыми являются изготовление либо хранение с целью распространения или рекламирования либо распространение, рекламирование, трансляция или публичная демонстрация порнографических материалов, печатных изданий, изображений, кино-, видеофильмов или сцен порнографического содержания, иных предметов порнографического характера.

Указанные действия, совершенные с использованием сети Интернет, иной сети электросвязи общего пользования либо выделенной сети электросвязи, являются квалифицирующим признаком, определенным ч. 2 ст. 343 УК, и за них предусмотрено наказание в виде лишения свободы на срок от двух до четырех лет.

Говоря об объективной стороне преступления, следует отметить, что под изготовлением порнографических материалов понимается как их создание, так и техническое воспроизведение (тиражирование). Способ изготовления определяется характером материального носителя, на котором воплощается порнографическое произведение. Им может быть

написание, рисование, видеозапись, фотосъемка, печатание, копирование и т. д. Внесение изменений или переделка существующих произведений с целью придания им порнографического характера также считается изготовлением.

Хранение порнографических материалов образуют любые действия, связанные с нахождением их во владении виновного (в помещении, тайнике, при себе, на накопителе на жестких магнитных дисках и т. д.).

Распространение порнографических материалов предполагает их передачу хотя бы одному лицу независимо от способа (сбыт, дарение, обмен и т. д.), срока (на постоянной основе или временно), возмездности (за плату или без нее) и иных обстоятельств.

Рекламирование порнографических материалов заключается в выставлении таких предметов для всеобщего обозрения либо сообщении информации о них неопределенному кругу лиц любым способом, например путем внесения данных о них в доступные для любого пользователя сайты сети Интернет или иной сети электросвязи.

Под публичной демонстрацией порнографических материалов понимается показ порнофильмов, обеспечивающий их просмотр, восприятие несколькими лицами.

Эффективное решение задач, определенных ст. 2 УК и ст. 7 УПК, возможно только при дальнейшем совершенствовании частных методик расследования отдельных видов (групп) преступлений с учетом основных принципов общих положений криминалистической методики. Все это требует от ученых-криминалистов углубленного исследования основополагающих проблем криминалистики, которые смогли бы расширить теоретическую базу разработки частных методик. Это становится особенно актуальным тогда, когда речь идет о преступлениях, методики расследования которых отсутствуют или не разработаны достаточно глубоко. В связи с этим возникает необходимость в определении их криминалистической характеристики как одного из элементов частной криминалистической методики, представляющего собой систему сведений о типичных криминалистически значимых признаках преступления, знание которых помогает при расследовании преступления.

Наиболее значимыми элементами криминалистической характеристики изготовления и распространения порнографических материалов являются личность потерпевшего, личность преступника, мотивы совершения преступления, способ совершения преступления, следовая картина.

Предложенный набор элементов криминалистической характеристики наиболее полно и всесторонне отражает содержание рассматриваемых

преступлений, позволяет детально изучить особенности их совершения и предложить наиболее эффективный механизм их расследования.

Потерпевшими в большинстве случаев являются женщины, как правило, в возрасте 16–30 лет, неработающие, имеющие низкий уровень образования. Если потерпевшими являются дети, то они в основном из неблагополучных семей, в которых низкий уровень дохода на одного члена семьи, родители злоупотребляют спиртными напитками и т. д. Потерпевшими также являются те, кто смотрит порнографию, так как это посягает на общественную нравственность.

Вместе с тем не всегда стоит сразу же признавать потерпевшими лиц, материалы с изображением которых размещены в сети Интернет. В отдельных случаях они могут приобретать статус свидетелей. Если же в ходе расследования будет установлено, что эти лица получали деньги за съемки, изначально отдавали себе отчет, чем они занимаются, то они являются соучастниками и их действия следует квалифицировать по соответствующим статьям УК.

Если в изготовлении порнографической продукции были задействованы дети, то необходимо рассматривать вопрос о признании их потерпевшими по соответствующим составам преступлений (развратные действия, насильственные действия, вовлечение в антиобщественную деятельность и т. д.).

Личность преступника по рассматриваемым преступлениям можно охарактеризовать с большой степенью условности. Как правило, это лица мужского пола в возрасте 18–35 лет с достаточным уровнем образования, ведущие нормальный образ жизни (не антиобщественный и аморальный), не злоупотребляющие спиртными напитками, имеющие постоянное место работы или обучающиеся.

Однако данные преступления могут совершить представлители абсолютно всех категорий граждан, причем даже не имея специального образования, а обладая всего лишь общими навыками работы на компьютере, имеющими дома персональный компьютер с выходом в сеть Интернет.

Можно выделить следующие ***мотивы*** совершения рассматриваемых преступлений:

– для удовлетворения личных потребностей;

– в целях совершения иных правонарушений (разглашение личных и (или) клеветнических сведений, с целью опозорить);

– в корыстных целях.

Центральным элементом криминалистической характеристики распространения порнографических материалов с использованием средств компьютерной техники в сети Интернет является способ его совершения. Дифференцируют эти способы в зависимости от мотивов совершения преступления.

Рассмотрим наиболее типичные ***способы*** совершения рассматриваемых преступлений.

Цель преступления – удовлетворение личных потребностей.

Практика расследования уголовных дел в Республике Беларусь по ст. 343, 343[1] УК позволяет к таким способам отнести создание пользователем, работающим в локальных сетях, директории для открытого доступа с содержащимися в ней порнографическими изображениями и размещение порнографических материалов в социальных сетях (без каких-либо корыстных целей).

Так, в 2009 г. следственными подразделениями Республики Беларусь было расследовано уголовное дело в отношении П., который, находясь у себя дома, сфотографировался в обнаженном виде, умышленно демонстрируя свои возбужденные гениталии, тем самым изготовил порнографическое изображение и, имея доступ к сети Интернет по месту жительства, разместил изготовленное порнографическое изображение в анкете знакомств на сайте intimby.net с рекламной надписью «с целью виртуального развлечения». Так он распространил и рекламировал порнографическое изображение, которое было доступно для любых пользователей сети Интернет и просмотрено ими 401 раз.

Цель преступления – совершение иных правонарушений (разглашение личных и (или) клеветнических сведений, с целью опозорить).

В качестве способов совершения таких преступлений можно привести ряд уголовных дел, расследованных следственными подразделениями Республики Беларусь.

Так, в 2010 г. в Бобруйске 46-летний мужчина познакомился с 16-летней школьницей. Ухаживал за ней, угощал дорогими спиртными напитками, забирал из школы на своем автомобиле. Однажды пригласил ее вместе с подружкой к себе домой. Одна из девушек после употребления спиртного быстро заснула. Тогда мужчина, раздев ее, сфотографировал обнаженную на телефон. Через две недели эти фотографии по цепочке были скопированы на телефоны многих знакомых как мужчины, так и школьницы[1].

В другом случае молодой человек после расставания с девушкой разместил в сети Интернет интимные фотографии последней с целью ее опозорить и прорекламировал ссылки по всему институту, где она училась.

Под эту же категорию подпадают и все «невинные шалости», связанные с работой в графических редакторах, например Photoshop, когда

[1] См. об этом: Фотографии голой школьницы две недели гуляли по всему Бобруйску [Электронный ресурс]. URL: http://news.rambler.ru/7955773.

совмещается фотография лица какой-либо девушки с фотографией порнографического содержания и впоследствии распространяется в сети Интернет, других сетях электросвязи.

Преступление совершается в корыстных целях.

Большинство рассматриваемых преступлений все же совершаются в корыстных целях, когда на изготовлении и распространении порнографии преступники пытаются заработать, занимаются распространением порнографических материалов, используя чужие труды, т. е. находят где-либо порнографическую продукцию и потом размещают ее в сети Интернет, локальных сетях. Хотя имеются и такие прецеденты, когда обвиняемый самостоятельно занимался организацией фотосъемки и видеозаписи.

В случае наличия у преступника корыстной цели преступления совершаются по следующим ***основным алгоритмам***.

1-й алгоритм совершения преступлений.

1. С порнографических сайтов злоумышленник копирует порнографические фото- и видеоматериалы.

2. Такие фото- и видеоматериалы сортируются, отбираются наиболее интересные либо по определенным порнографическим тематикам и группируются в архивы (архивируются). Архивация производится для того, чтобы сжать размер файла (при загрузке расходуется меньше трафика). Из всех фотоизображений в архиве отбираются наиболее качественные фотоснимки, которые используются в качестве рекламы всего архива на страницах различных форумов и т. д. Из видеоматериалов выбираются качественные скриншоты эпизодов видеофильма, которые также используются в качестве рекламы всего фильма. Часто эта работа уже проведена, и злоумышленник только копирует фото- и видеоматериалы с уже отобранными для рекламы фотоснимками и скриншотами.

3. Злоумышленник регистрируется на каком-либо файлообменнике (сайт, предназначенный для обмена файлами различных форматов между пользователями, на котором одни размещают файлы, а другие их просматривают либо копируют на свой компьютер). При регистрации на подобном сайте злоумышленник создает свой аккаунт, для доступа к которому используются уникальные логин и пароль. Регистрация на файлообменниках бесплатная. Основное правило файлообменника: пользователь, который разместил какой-либо файл на сервере файлообменника, получает определенную прибыль в виде электронных денег (в основном WebMoney) за определенное количество просмотров размещенного файла сторонними пользователями. Следовательно, чем популярнее файл, который размещается на файлообменнике, тем, соответственно, большее количество пользователей его просмотрят и больше заработает тот, кто такой файл разместил[1].

4. С использованием зарегистрированного аккаунта злоумышленник размещает на сервере файлообменника заранее подготовленные архивы с порнографическими фото- и видеоматериалами. Каждый такой размещенный архив имеет ссылку, которую в автоматическом режиме формирует система файлообменника. Данная ссылка является электронным адресом размещения архива, состоит из адреса сервера самого файлообменника и случайно сгенерированного из цифр и букв имени файла. Соответственно, при переходе по данной ссылке можно просмотреть (скопировать) размещенный там архив.

5. Затем злоумышленник рекламирует свой архив с порнографическими фото- и видеоматериалами путем размещения ссылки для его просмотра на различных интернет-форумах соответствующей порнографической тематики (на некоторых из таких форумов регистрация обязательна, на некоторых не требуется); в спам-книгах – на своеобразных досках объявлений, где для подачи объявления необходимо заполнить определенную форму с графами для различной информации (регистрация не требуется); на иного рода интерактивных досках объявлений либо на лично созданных сайтах. Вместе со ссылкой размещаются определенный рекламный текст, в котором описывается содержимое архива, а также размещаются заранее подобранные рекламные фотоснимки и скриншоты, иллюстрирующие наиболее качественные порнографические фото- и видеоматериалы из архива.

6. При копировании сторонними пользователями размещенного злоумышленником архива с порнографическими материалами файлообмен-

[1] Из-за большого распространения и популярности порнографии в сети Интернет именно порнографические файлы (фото- и видеоматериалы) чаще всего размещаются и просматриваются через файлообменники. Соответственно, наибольшую прибыль получает именно тот пользователь, который размещает файлы именно порнографического содержания, причем чем файл качественнее и реже встречается, тем больше пользователей его просмотрят и больше заработает лицо, его разместившее. Различные файлообменники и различные тарифные планы позволяют получить различную прибыль – от 5 до 25 долларов США (в эквиваленте электронным титульным знакам) за 1 000 просмотров одного архива (в архиве может быть от одного до неопределенного количества файлов). Прибыль также зависит от страны, из которой пользователь скачал файл. Например, файлообменник depositfiles.com платит 15 долларов США за 1 000 просмотров из стран Евросоюза, 20 долларов США – за 1 000 просмотров из США. Сами же файлообменники зарабатывают на том, что предоставляют кроме бесплатного скачивания, которое имеет различные ограничения по времени и количеству скачиваний, также платное скачивание, которое не имеет ограничений и поэтому более удобно. Для получения возможности такого скачивания файлообменники предлагают отправить платное СМС, оплатить электронными деньгами и т. п. В сети Интернет встречается огромное количество ссылок на возможность заработка с помощью файлообменников.

ник в автоматическом режиме зачисляет на его электронный кошелек, указанный при регистрации аккаунта, определенные денежные средства в качестве платы за копирование размещенного архива. Данные денежные средства в последующем обналичиваются злоумышленником путем снятия наличных денежных средств.

2-й алгоритм совершения преступлений.

Второй способ совершения преступлений сходен с описанным выше, за исключением того, что злоумышленник распространяет порнографические материалы не через файлообменники, а другим путем. Подготовив порнографические материалы, злоумышленник рекламирует их на различных сайтах и в социальных сетях, предлагая за определенную плату направить их адресату. После этого злоумышленник регистрирует электронный кошелек для перевода электронных денег.

Желающие получить порнографическую продукцию перечисляют на этот кошелек заранее оговоренную денежную сумму, и после ее получения злоумышленник со своего электронного почтового ящика направляет по электронной почте архив с фото- и видеоматериалами адресату.

3-й алгоритм совершения преступлений.

Назвать приведенный ниже алгоритм типичным не представляется возможным, поскольку для Республики Беларусь он является единичным случаем, однако привести такой пример считаем необходимым.

В 2011 г. следственными подразделениями Республики Беларусь расследовалось уголовное дело по ст. 343 УК. Был установлен факт организации веб-студии и проведения онлайн-трансляций сомнительного содержания. Перед веб-камерой, находившейся в такой «студии», располагались девушки. Любой желающий, знавший адрес соответствующего сайта, связывался с организаторами, оплачивал предлагаемые услуги и наблюдал за девушками со своего домашнего компьютера. Естественно, что девушки выполняли все пожелания клиентов – раздевались и т. д.

При распространении порнографических материалов в сети Интернет остается определенная ***следовая картина*** в виде идеальных и материальных следов.

Среди идеальных следов наиболее значимыми являются:

– показания потерпевшего;

– показания свидетелей, которыми могут выступать родственники потерпевшего, пользователи сети Интернет, видевшие размещенные порнографические материалы, сотрудники органов внутренних дел, выявившие соответствующее преступление;

– показания подозреваемого, обвиняемого.

Материальные следы данного вида преступления будут находиться на компьютере обвиняемого и на серверах в сети Интернет. К ним относятся:

– порнографические изображения на интернет-сайтах;

– рекламные объявления о предоставлении порнографических материалов;

– накопители на жестких магнитных дисках с компьютера, которым пользовался обвиняемый, и т. д.

В качестве поводов к возбуждению уголовного дела, как правило, выступают:

– непосредственное обнаружение органом уголовного преследования сведений, указывающих на признаки преступления;

– заявления граждан;

– сообщения в средствах массовой информации.

Наиболее распространенным является первый из указанных поводов. Материалы проверки собирают в основном сотрудники подразделений по наркоконтролю и противодействию торговле людьми, но могут и иных оперативных подразделений при поступлении к ним первичной информации о преступлении (например, материалы проверки о преступлениях, предусмотренных ч. 2, 3 ст. 343^1 УК, собирает управление по раскрытию преступлений в сфере высоких технологий).

Расследование уголовных дел о распространении порнографических материалов с использованием средств компьютерной техники в сети Интернет, локальных сетях протекает в трех следственных ситуациях, характерных для первоначального этапа:

– имеются данные, указывающие на признаки преступления, сведения о лицах, причастных к его совершению, отсутствуют;

– имеются данные, указывающие на признаки преступления, сведения о лицах, причастных к его совершению, неполные или неточные;

– имеются данные, указывающие на признаки преступления, при этом установлено лицо, его совершившее.

В качестве исходного примем положение, когда оперативный сотрудник (следователь) находится в ситуации информационной неопределенности, т. е. имеется информация о признаках преступления, предусмотренного ст. 343, 343^1 УК, – в сети Интернет обнаружено изображение (видеоролик), содержащее признаки порнографии.

Первое, что необходимо сделать, – зафиксировать выявленные на данный момент признаки противоправного деяния, т. е. путем проведения оперативно-розыскных мероприятий либо следственных действий обеспечить сохранность информации о том, какие порнографические материалы и где они были обнаружены. Фиксация доказательств в таком случае производится, как правило, путем проведения оперативно-розыск-

ного мероприятия «исследование предметов и документов» либо при проведении следственного действия «осмотр предметов и документов».

После того как информация о размещении в сети Интернет материалов, предположительно являющихся порнографическими, зафиксирована в протоколе соответствующего оперативно-розыскного мероприятия (следственного действия), а копии данных изображений (видеороликов) записаны на внешний машинный носитель информации, оперативный сотрудник (следователь) начинает сбор сведений о личности преступника (лица, которое распространило порнографические материалы в сети).

Если порнографические материалы обнаружены на специализированном сайте (специально созданном для распространения порнографии), необходимо установить конкретный сервер, на котором данный сайт расположен. Определение места расположения сервера осуществляется с использованием интернет-сервиса whois (whois.net, 2ip.ru), предназначенного для получения информации о доменных именах и IP-адресах (Internet Protocol – сетевой адрес узла в компьютерной сети).

Если порнографические материалы обнаружены в социальных сетях, то следственная ситуация становится относительно определенной. В данном случае у оперативного сотрудника (следователя) появляется неполная или неточная информация о личности преступника. В качестве такой информации выступают: никнейм (прозвище в сети) пользователя, на страничке которого размещены порнографические материалы; адрес его электронной почты; имя и фамилия пользователя (которые не всегда достоверны); номер интернет-пейджера; сведения о связях проверяемого лица с другими пользователями сети.

В данной ситуации после проведения осмотра интернет-страницы, на которой размещены порнографические материалы, направляется запрос администрации сайта с требованием заблокировать доступ к порнографическим материалам, обеспечить их сохранность, а также представить имеющуюся информацию о пользователе, зарегистрировавшем интересующий аккаунт. В полученном ответе могут содержаться сведения о сессиях, проведенных проверяемым лицом на сайте, а также IP-адрес, с которого был осуществлен доступ к серверу. После этого при помощи интернет-сервиса whois производится проверка IP-адреса с целью установления поставщика интернет-услуг, клиентом которого является проверяемое лицо. Далее направляется запрос интернет-провайдеру с требованием представить информацию о том, кому выделялся конкретный IP-адрес в определенный период времени, а также полную информацию об указанном лице, имеющуюся у оператора электросвязи. В необходимых случаях может проводиться оперативно-розыскное мероприятие

«контроль в сетях электросвязи» с целью установления дополнительных эпизодов преступной деятельности проверяемого лица.

Еще одним способом получения информации о лице, распространившем в сети порнографическую продукцию, является установление места проведения съемок видеоролика (изображения) либо лица, участвовавшего в изготовлении порнографических материалов в качестве актера (модели). Довольно часто этот способ используется при расследовании уголовных дел о преступлениях, предусмотренных ст. 343[1] УК. В данном контексте представляет интерес созданная в 2009 г. Международная база данных изображений сексуальной эксплуатации детей (the International Child Sexual Exploitation (ICSE) image database)[1]. Она реализуется под эгидой Интерпола и направлена на повышение количества идентифицированных и спасенных жертв сексуального насилия, предусматривает прямой доступ к базе данных в режиме реального времени (посредством использования I-24/7) любого авторизованного пользователя из государства – члена Интерпола. Указанная база данных содержит массив изображений, обнаруженных и изъятых при производстве расследования правоохранительными органами государств – участников данной международной организации. Для получения сведений о следователе, расследовавшем уголовное дело, месте и времени совершения преступления необходимо разместить обнаруженные порнографические материалы в указанной базе и произвести поиск соответствий. В случае обнаружения совпадений программа выдаст сведения, указанные выше.

Кроме того, возможен поиск актера (модели) по каким-либо особым приметам (особенности телосложения, татуировки, одежда и т. д.).

Так, полиция Молдовы расследовала уголовное дело о распространении в сети Интернет порнографических материалов с изображением несовершеннолетней. На некоторых фотоснимках девочка была одета в национальный молдавский костюм. Следователями была выдвинута версия о том, что она занимается в школе национального танца. Через некоторое время один из педагогов кишиневской школы танца опознал в девочке свою ученицу, а в мужчине, участвовавшем в съемках, ее отчима.

В другом случае бюро специальных технических мероприятий полиции России выявило в сети Интернет порнографические изображения несовершеннолетней. На одном из фотоснимков девочка стояла в коридоре многоквартирного дома, где на стене были указаны номера телефонов управляющей компании жилищно-коммунального хозяйства. Таким образом был установлен примерный адрес, где произошла фотосессия, а после проведения оперативно-розыкных мероприятий – и сама модель.

[1] Подробнее см.: Victim identification [Электронный ресурс]. URL: https://www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification

Рассмотрим специфические особенности проведения отдельных следственных действий, наиболее характерных для расследования уголовных дел рассматриваемой категории.

Целью ***осмотра места происшествия*** является установление конкретного средства компьютерной техники, выступающего в качестве предмета и (или) орудия совершения преступления и имеющего следы преступной деятельности. При производстве следственного действия целесообразно использовать тактический прием «от центра – к периферии», где центром (отправной точкой осмотра места происшествия) являются средства компьютерной техники, находящиеся на месте осмотра.

Специфическими объектами осмотра по делам данной категории являются средства компьютерной техники, а также машинные носители информации. Одним из требований практики является обязательное изъятие всех средств компьютерной техники и носителей информации, обнаруженных при производстве осмотра.

При осмотре места происшествия в состав следственно-оперативной группы в зависимости от конкретной следственной ситуации могут входить следующие лица:

– следователь, специализирующийся на расследовании уголовных дел рассматриваемой категории, – руководитель следственно-оперативной группы;

– эксперт-криминалист, знающий особенности работы со следами преступлений данной категории;

– специалист по средствам компьютерной техники;

– сотрудник оперативного подразделения (управления по наркоконтролю и противодействию торговле людьми или управления по раскрытию преступлений в сфере высоких технологий);

– специалист по сетевым технологиям (в случае наличия на месте происшествия периферийного оборудования удаленного доступа или локальной компьютерной сети);

– специалист по системам связи (при использовании каналов электросвязи для дистанционной передачи данных);

– оперативные сотрудники иных оперативных подразделений органов внутренних дел;

– участковый инспектор милиции, обслуживающий данную территорию;

– сотрудник Департамента охраны (в случае, если место происшествия или средства компьютерной техники, находящиеся на нем, являются охраняемыми объектами).

При необходимости для участия в осмотре места происшествия могут быть приглашены и другие не заинтересованные в деле специалисты, знающие специфику работы осматриваемого объекта (инженеры-электрики, специалисты спутниковых систем связи, операторы компьютерных систем и сетей – сотовых, пейджинговых, Интернет и др.).

Рассматриваемое следственное действие должно быть заблаговременно подготовлено и детально спланировано. Для этого необходимо:

– с учетом сложившейся следственной ситуации наметить круг лиц, участвующих в осмотре;

– определить последовательность действий лиц при осмотре места происшествия;

– пригласить соответствующих квалифицированных специалистов;

– перед началом осмотра разъяснить цели проведения следственного действия и задачи, стоящие перед специалистами, а также их права и обязанности;

– провести подбор и инструктаж понятых, в качестве которых целесообразнее привлекать лиц, обладающих минимально необходимыми знаниями в области средств компьютерной техники и компьютерных технологий, разъяснить их права и обязанности.

По прибытии на место происшествия следователь (далее по тексту – следователь или иное уполномоченное лицо, производящее осмотр) должен:

– удалить с места происшествия всех посторонних лиц и организовать его охрану, если этого не было сделано. Обязательной охране подлежат такие объекты, как территория места происшествия, все средства компьютерной техники, находящиеся на территории (в помещении), пункты отключения электропитания средств компьютерной техники, находящиеся в здании (в организации, на территории). Необходимо отметить, что к изменению или уничтожению информации (следов) может привести не только использование устройств ввода и целеуказания (клавиатура, мышь), но и включение-выключение средств компьютерной техники или разрыв соединения между ними. Поэтому, если на момент производства следственного действия какие-либо средства компьютерной техники и иные электротехнические приборы и оборудование были включены или выключены, они должны оставаться в таком состоянии до момента окончания осмотра их специалистом;

– опросить находящихся в помещении лиц (операторов средств компьютерной техники) об изменениях, внесенных в обстановку, категории обрабатываемой информации (общедоступная или конфиденциальная), а также о действиях лиц, работавших за конкретными средствами компьютерной техники. Вопросы необходимо конкретизировать по мере детального осмотра места происшествия, поиска следов и других вещественных доказательств.

К протоколу осмотра прилагаются план или схема места происшествия, принципиальная схема соединения средств компьютерной техники между собой и с каналами электросвязи (со спецификацией и расшифровкой условных обозначений), фото-, видеопленка или магнитный носитель информации, распечатка информации.

Обыск проводится в соответствии с требованиями ст. 208, 210 УПК и общими криминалистическими рекомендациями проведения данного следственного действия. При обнаружении средств компьютерной техники, машинных носителей информации и иных объектов их изъятие проводится в соответствии с правилами, описанными выше.

Неотъемлемым следственным действием при расследовании уголовных дел о преступлениях указанной группы является ***осмотр информации, хранящейся на машинных носителях информации,*** – компьютерной информации. Осмотр компьютерной информации, несомненно, является одной из форм использования специальных знаний при проведении следственных действий, к которым можно отнести:

– использование следователем собственных специальных знаний (в данном случае это специальные знания в области информатики, радиоэлектроники, программирования);

– участие специалиста в проведении отдельных следственных действий (осмотр, обыск, выемка, допрос);

– назначение и производство судебных экспертиз (компьютерно-технических и др.).

В настоящее время основной проблемой при использовании специальных знаний в расследовании преступлений в сфере высоких технологий является то, что проведение компьютерно-технических экспертиз является достаточно трудоемким процессом, что влечет большую продолжительность их производства. Постоянный рост количества преступлений в сфере высоких технологий позволяет предположить, что сроки производства таких экспертных исследований будут только расти. С учетом сложившейся ситуации особую роль играют иные формы использования специальных знаний в расследовании преступлений.

В практической деятельности следователь, как правило, самостоятельно проводит осмотр компьютерной информации с целью обнаружения следов преступной деятельности (наличие порнографических материалов, переписки и т. д.). Такой осмотр желательно проводить с участием специалиста, при этом нельзя использовать выражение «порнографические изображения», следует использовать термин «изображения, которые предположительно являются порнографическими».

Анализ материалов уголовных дел, возбужденных по признакам преступлений, предусмотренных ч. 2 ст. 343 и ч. 2 ст. 343^1 УК, показал,

что ход и результаты такого осмотра в настоящее время оформляются протоколом осмотра предметов и документов (таким образом, компьютерная информация выступает в качестве либо документов, либо следов преступной деятельности). С учетом того, что ст. 6 УПК не содержит определений ни предметов, ни документов, такой подход видится правильным. Осмотру в данном случае подлежат:

– машинные носители информации компьютеров, изъятых у подозреваемого, – в целях обнаружения порнографических материалов, следов деятельности лица в сети Интернет, иной криминалистически значимой информации;

– удаленные ресурсы, несущие следы преступной деятельности либо на которых производилось размещение порнографической продукции;

– иные предметы и документы, имеющие значение для расследования уголовного дела, обладающие свойствами хранения компьютерной информации: внешние HDD (малогабаритные переносные накопители на жестких магнитных дисках), Flash USB Drive (флэш-накопитель, флэшка), Flash-memory (флэш-память, карта памяти), оптические (лазерные) диски, «карманные компьютеры» (Personal Data Assistant, КПК), оконечные устройства сотовой связи (телефоны, смартфоны и т. д.), электронные книги, цифровые фото- и видеокамеры, MP3-плееры, игровые приставки, GPS-навигаторы и т. д.

Все следы, обнаруженные следователем при производстве осмотра, должны сопоставляться с иными доказательствами, собранными по уголовному делу (например, с результатами снятия информации с технических каналов связи, осмотров удаленных ресурсов, осмотров иных средств компьютерной техники и машинных носителей информации, а также иных оперативно-розыскных мероприятий и следственных действий), что прямо предусмотрено ч. 2 ст. 103 УПК. Выводы следователя могут быть изложены в справке о результатах предварительного расследования по уголовному делу, иных документах (рапортах, справках).

Однако не все следователи обладают достаточными знаниями, умениями и навыками проведения осмотра компьютерной информации и средств компьютерной техники. В таком случае к осмотрам обязательно надо привлекать соответствующих специалистов. Специалисты в таких случаях указывают следователю на конкретные каталоги и файлы, содержание которых необходимо отразить в протоколе. После проведения осмотра следователь допрашивает специалиста, который в процессе допроса поясняет, как были обнаружены те или иные следы, по каким признакам и какими средствами они были выявлены, о какого рода деятельности пользователя исследуемого средства компьютерной техники они свидетельствуют и т. д.

При осуществлении ***допроса подозреваемого*** помимо выяснения общих вопросов, предлагаемых тактикой его проведения, необходимо детально конкретизировать:

– цели и мотивы совершения преступления;

– умысел лица;

– источник получения им порнографических материалов, которые впоследствии были распространены;

– способ совершения преступления.

Следует иметь в виду, что нередко в ходе допросов подозреваемые используют лексику, которая применяется ими в общении с пользователями средств компьютерной техники.

Проведение других следственных и иных процессуальных действий подчинено общим требованиям организации их производства и ярко выраженной принципиальной специфики не имеет.

В общих чертах обрисовать алгоритм расследования преступлений можно следующим образом:

– проведение осмотра места происшествия (места обнаружения преступления);

– назначение и производство искусствоведческой экспертизы;

– установление лица, разместившего порнографические материалы в сети;

– обыск в жилище подозреваемого, изъятие машинных носителей информации и средств компьютерной техники;

– осмотр машинных носителей информации и средств компьютерной техники, изъятых у подозреваемого, с целью обнаружения порнографических материалов, а также иных следов преступной деятельности;

– проведение допроса;

– назначение и производство компьютерно-технической экспертизы;

– изъятие других вещественных доказательств, допросы свидетелей, проведение иных следственных и процессуальных действий.

Эти действия направлены на процессуальное собирание (обнаружение, фиксацию, изъятие) доказательств причастности подозреваемого к совершению преступления. Набор действий следователя в данных ситуациях во многом имеет отработанный на практике стандартный характер (с точки зрения организации и тактики проведения следственных действий).

Назначение экспертных исследований, кроме искусствоведческой экспертизы, является чаще всего факультативным и зависит от конкретной ситуации и экспертных возможностей региона.

Вопросы на экспертное исследование следует ставить лаконично, они должны иметь однозначную трактовку. Если предполагается вынесение сложного вопроса, его рекомендуется разбить на ряд простых.

При постановке вопроса следует предполагать только однозначный ответ эксперта на поставленный вопрос (в идеальном случае – «да» или «нет»). Неопределенные ответы эксперта неприемлемы (например, корректным является ответ эксперта «отсутствует» или «не содержит»; ответ эксперта «не выявлено» не корректен, так как подразумевает возможность дальнейшего исследования этого же объекта, т. е. эксперт, приходя к такому выводу, фактически признает, что исследование им проведено не в полном объеме, что недопустимо).

На объектах, содержащих порнографические материалы, могут быть обнаружены и традиционные криминалистические следы: пальцев рук, иных участков тела человека, одежды, специальных химических веществ (при их использовании, например, в результате проведения проверочной закупки), объекты, содержащие ДНК. Такие объекты необходимо исследовать в первую очередь. Не исключены также и иные исследования, например исследование материалов документов (бумаги, красителей и т. д.), почерковедческие исследования.

Согласно ст. 343, 343[1] УК определим объекты (табл. 1) и виды (табл. 2) возможного экспертного исследования[1].

Таблица 1

Объекты экспертного исследования

Общий объект исследования	Непосредственный объект исследования
Порнографические материалы	Печатные издания (в том числе и выполненные на принтерах и средствах множительной техники). Рисованные изображения. Видеоматериалы, иные материалы на электронных носителях информации, в том числе памяти компьютеров, мобильных телефонов и т. д.
Объекты, несущие информацию об изготовлении порнографических материалов	Видеозаписи. Материалы на электронных носителях информации, в том числе памяти компьютеров, мобильных телефонов и т. д. (видео-, аудиозаписи, графические файлы, текстовые файлы), содержащие исходные данные для изготовления порнографических материалов или упаковок для них – компьютерная графика, видеозаписи, тексты и пр.; объекты технического характера, связанные с тиражированием порнографических материалов.

[1] См.: Бугаев К.В. Экспертное сопровождение расследования преступлений, предусмотренных ст. 242 УК РФ (Незаконное распространение порнографических материалов или предметов) // Законодательство и практика. 2010. № 1. С. 30–31.

Окончание табл. 1

Общий объект исследования	Непосредственный объект исследования
	Вещная обстановка, имеющая отношение к фото-, видеосессиям, связанным с изготовлением порнографических материалов. Информация в памяти людей
Объекты, несущие информацию, свидетельствующую о наличии цели распространения или рекламирования порнографических материалов при их изготовлении	Материальные носители порнографических материалов, имеющие значительные объемы. Материалы, указывающие на цели изготовителей: записи оперативной видео-, аудиозаписи; бумажные и электронные документы, отражающие планы изготовителей. Информация в памяти людей
Объекты, несущие информацию о распространении и рекламировании порнографических материалов	Объекты, аналогичные указанным в предыдущих пунктах. При определении объектов исследования следует обращать внимание на распространение информации о порнографических материалах (в том числе о их местонахождении) в виде рекламных листков, стендов, почтовых рассылок, рассылок по электронной почте, гиперссылок в компьютерных сетях, иных графических и текстовых сообщениях
Объекты, несущие информацию о торговле порнографическими материалами	Электронные документы и документы на бумажных носителях, подтверждающие факт такой сделки. Информация в памяти людей

Таблица 2

Виды экспертных исследований

Объект экспертного исследования	Вид экспертизы	Задачи экспертного исследования
Бумажные и подобные им носители, возможно содержащие порнографическую информацию	Искусствоведческая	Установление наличия признаков порнографических материалов
	Портретная	Установление конкретных лиц, изображенных на фото-, видеоматериалах
	Автороведческая	Установление автора текста

Продолжение табл. 2

Объект экспертного исследования	Вид экспертизы	Задачи экспертного исследования
Видео-, фотоматериалы, возможно содержащие порнографическую информацию	Искусствоведческая	Установление наличия признаков порнографических материалов
	Фоноскопическая. Фототехническая	Установление аппаратуры, посредством которой выполнены материалы. Установление технических характеристик этих материалов
Электронные носители, возможно содержащие порнографическую информацию	Компьютерно-техническая	Установление факта и места наличия определенных материалов и предоставление возможности доступа к ним и характера такого доступа (открытого, частично закрытого, закрытого)
Объекты технического характера, связанные с тиражированием порнографических материалов	Инженерно-технологическая (с привлечением специалистов в области полиграфии, средств аудио-, видеозаписи)	Установление того, что обнаруженные технические объекты являются частью определенного технологического процесса
Личность преступника	Медицинская экспертиза физического лица (привлечение специалиста-сексолога)	Установление патологий сексуального характера
	Психологическая	Исследования на полиграфе (с целью получения скрываемой информации об изготовлении, распространении, рекламировании, торговле порнографическими материалами)
	Комплексная психолого-психиатрическая	Установление эффекта (результата) взаимодействия болезненных психопатологических) и небольшенных (возрастного, ситуационного, эмоционального, личностного) психических факторов и определение на основе

Окончание табл. 2

Объект экспертного исследования	Вид экспертизы	Задачи экспертного исследования
		учета этого системного качества наиболее полной и точной меры их влияния на характер психического отражения, рефлексии и регуляции поведения данного лица в интересующий период. Установление особенностей психики в плане наличия поведенческих отклонений сексуального характера

Рассмотрим некоторые вопросы основного для рассматриваемого состава преступления исследования – *искусствоведческой экспертизы* (назначение данной экспертизы является обязательным по делам данной категории, она должна проводиться до возбуждения уголовного дела), которая предполагает решение комплекса задач, связанных с анализом и оценкой художественных произведений с целью их атрибуции, определения историко-культурной и материальной ценности, идейного содержания, а также разрешения частных вопросов, требующих выяснения при характеристике подобных произведений.

Основной вопрос, разрешаемый искусствоведческой экспертизой: является ли изображение (видеоролик и т. д.) порнографическим или нет?

В Республике Беларусь он решается только экспертами. Для этих целей в соответствии с постановлением Совета Министров Республики Беларусь от 22 октября 2008 г. № 1571 «Об экспертных комиссиях по предотвращению пропаганды порнографии, насилия и жестокости» создана и постоянно действует Республиканская экспертная комиссия по предотвращению пропаганды порнографии, насилия и жестокости (далее – РЭК), а также соответствующие областные комиссии, в состав которых входят представители государственных органов и организаций, специалисты в области культуры, искусства, медицины, образования, юриспруденции, информационных технологий и иных сфер деятельности.

Следует отметить, что в настоящее время фактически решен вопрос о дополнении полномочий данной комиссии. Расширение состава комиссий связано с тем, что в компетенцию РЭК не входит решение вопросов о возрасте актеров (моделей), принимавших участие в создании порнографических материалов. Ответ на данный вопрос является очень актуальным и влияет на квалификацию деяний подозреваемых лиц.

Так, максимальный срок лишения свободы, установленный ч. 2 ст. 343 УК (распространение порнографических материалов с использованием глобальной компьютерной сети Интернет), составляет 4 года, в то время как ч. 2 ст. 343^1 УК (распространение материалов порнографического характера с изображением несовершеннолетнего с использованием глобальной компьютерной сети Интернет) – до 8 лет с конфискацией имущества, а ч. 3 ст. 343^1 УК (распространение материалов порнографического характера с изображением заведомо малолетнего с использованием глобальной компьютерной сети Интернет) – до 13 лет с конфискацией имущества.

Именно для решения вопроса о возрасте лица, участвовавшего в изготовлении порнографической продукции, в состав РЭК входят педиатры, детские психологи, педагоги.

Кроме того, одной из проблем проведения искусствоведческой экспертизы является отсутствие какой-либо методики проведения данного исследования. При даче оценки тем или иным объектам, представленным на экспертизу, члены РЭК руководствуются в основном своим внутренним убеждением, а также положениями, изложенными в нормативных правовых актах Республики Беларусь.

Далее рассмотрим проблемные вопросы назначения компьютерно-технических экспертиз, как наиболее часто встречающихся при производстве расследования уголовных дел о распространении порнографических материалов в сети Интернет.

В данном случае используются специальные знания в следующих областях: электронике, электротехнике, информационных системах и процессах, радиотехнике и связи, вычислительной технике (в том числе программировании) и автоматизации. Существуют три вида компьютерно-технической экспертизы: аппаратная, программно-информационная, сетевая.

При производстве судебной *аппаратной экспертизы* как вида компьютерно-технической экспертизы решаются в основном следующие задачи:

– определение вида (типа, марки), свойств аппаратного средства, а также его технических и функциональных характеристик для решения определенных функциональных задач (например, обработки графических изображений с высоким разрешением);

– определение фактического состояния и исправности аппаратного средства, наличия физических дефектов;

– определение структуры механизма и обстоятельств события по его результатам за счет использования выявленных аппаратных средств как по отдельности, так и в комплексе в составе компьютерной системы;

– установление причинной связи между использованием конкретных возможностей аппаратных средств и результатами их применения;

– определение условий (обстановки) применения аппаратных средств, восстановление хронологической последовательности их использования, места действия и функционирования.

Примером аппаратной экспертизы является изучение возможностей применения нетипичных или нештатных (например, в случае удара или внезапного отказа) способов исследования носителей данных (чаще всего жестких дисков) с целью извлечения криминалистически значимой информации, хранящейся на них.

При проведении *программно-информационной экспертизы* (компьютерно-технической экспертизы программных объектов) могут решаться следующие экспертные задачи:

– определение основных характеристик операционной системы;

– выявление и исследование функциональных свойств, а также настроек программного обеспечения, времени его инсталляции;

– определение фактического состояния программного объекта, состава соответствующих ему файлов, их параметров (объемы, даты создания, атрибуты), способов ввода-вывода информации, наличия или отсутствия каких-либо отклонений от типовых параметров (например, недокументированных функций);

– выявление признаков отношения программного обеспечения к системному или прикладному и т. д.;

– диагностирование алгоритма программного продукта, видов использованных при его разработке инструментальных средств, а также типов поддерживаемых аппаратно-программных платформ;

– установление первоначального состояния программы (например, при начальной инсталляции) и выявление возможных последующих изменений;

– определение целей и условий изменения свойств и состояния программного обеспечения (преднамеренное изменение каких-либо функций, конфигурирование на конкретную аппаратную среду и др.), установление способа осуществления изменений в программе (например, воздействием вредоносной программы, ошибками программной среды, путем несанкционированного доступа);

– определение свойств и состояния программы по ее отображению в обрабатываемых данных (по содержанию служебных, системных файлов), соответствия обеспечивающих аппаратных средств;

– выявление структуры механизма события по результатам работы программного обеспечения и в динамике;

– установление причинной связи между действиями пользователя компьютерной системы в отношении программного обеспечения и наступившими последствиями.

Кроме указанных задач при проведении программно-информационной экспертизы могут решаться идентификационные задачи, связанные с индивидуальным отождествлением оригинала программы (инсталляционной версии) и ее копии на машинных носителях информации компьютерной системы, установлением групповой принадлежности программного обеспечения по общим признакам, выявлением частных признаков программы, позволяющих впоследствии идентифицировать ее авторство, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы. Также в рамках экспертного исследования программных средств могут устанавливаться признаки контрафактности представленных на экспертизу информационно-программных продуктов.

Для *сетевой экспертизы* характерна следующая группа экспертных задач:

– определение свойств и характеристик аппаратного средства и программного обеспечения; установление места, роли и функционального предназначения исследуемого объекта в сети (например, для программного средства – в отношении к сетевой операционной системе; для аппаратного средства – в отношении к серверу, рабочей станции, активному сетевому оборудованию и т. д.);

– выявление свойств и характеристик вычислительной сети, установление ее архитектуры, конфигурации, выявление установленных сетевых компонентов, организации доступа к данным;

– определение соответствия выявленных характеристик типовым для конкретного класса средств сетевой технологии; определение принадлежности средства к серверной или клиентской части приложений;

– определение фактического состояния и исправности сетевого средства, наличия физических дефектов, состояния системного журнала, компонентов управлением доступа;

– установление первоначального состояния вычислительной сети в целом и каждого сетевого средства в отдельности, возможного места покупки (приобретения), уточнение изменений, внесенных в первоначальную конфигурацию (например, добавление дополнительных сетевых устройств, устройств расширения на сервере либо рабочих станциях и пр.);

– определение причин изменения свойств вычислительной сети (например, по организации уровней управления доступом; установление факта нарушения режимов эксплуатации сети, фактов (следов) использования внешних («чужих») программ и т. п.);

– определение свойств и состояния вычислительной сети по ее отображению на машинных носителях информации (например, RAID-массивы (англ. Redundant Array of Independent Disks – избыточный массив независимых дисков – технология виртуализации данных, которая объединяет несколько дисков в логический элемент для повышения производительности); жесткие диски, CD-ROM и т. п.);

– определение структуры механизма и обстоятельств события в сети по его результатам (например, сценария несанкционированного доступа, механизма распространения в сети вредоносных функций и т. д.);

– установление причинной связи между использованием конкретных аппаратно-программных средств вычислительной сети и результатами их применения.

В качестве общей рекомендации при назначении компьютерно-технических экспертиз следует сказать, что конкретный перечень и формулировку вопросов с учетом обстоятельств дела целесообразно согласовывать с экспертами соответствующих подразделений Государственного комитета судебных экспертиз Республики Беларусь.

7. ОРГАНИЗАЦИЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Преступления против информационной безопасности юридически закреплены в гл. 31 УК.

Информационная безопасность согласно Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. Жизненно важными интересами могут выступать (в контексте квалификации противоправных деяний) обеспечение информационных потребностей личности, общества и государства во всех сферах их жизнедеятельности, обеспечение безопасности информационных систем и сетей связи.

Из заглавия ст. 352 УК «Неправомерное завладение компьютерной информацией» (и других статей гл. 31) следует, что правоприменителя интересует не просто информация, а один из ее видов – компьютерная информация. Поскольку форма компьютерной информации цифровая, т. е. данные представлены последовательностью всего двух знаков (0 и 1), то данные в любой другой форме – результат интерпретации непосредственно компьютерных данных. Это важно как для правильной квалификации и юридически грамотного описания состава преступления, так и для определения достоверности и достаточности доказательств, получаемых в результате осмотра носителей информации.

При классификации способов совершения криминальных деяний в сфере информационной безопасности в качестве системообразующего признака следует выделить направленность преступных деяний, т. е. ту цель, которую преследует преступник при совершении противоправного деяния.

При ***классификации способов совершения преступлений*** в сфере информационной безопасности выделяют следующие их группы:

– способы, направленные на несанкционированный доступ к информации в компьютерной системе, сети или на машинном носителе (компьютерной информации);

– способы, направленные на модификацию информации в компьютерной системе, сети или на машинном носителе;

– способы, направленные на уничтожение (блокирование) информации в компьютерной системе, сети или на машинном носителе или их самих;

– способы, направленные на неправомерное завладение компьютерной информацией;

– способы, связанные с незаконным оборотом программных или аппаратных средств, предназначенных для получения несанкционированного доступа к компьютерной информации, либо вредоносных программ;

– способы, направленные на нарушение правил эксплуатации компьютерной системы или сети;

– комплексное использование способов.

Первая группа способов охватывает всю совокупность преступных действий, направленных на *несанкционированный доступ к компьютерной информации*. При этом под несанкционированным понимается доступ к данной информации лица, которое не имеет на него права либо имеет право на доступ к данной информации, однако осуществляет его помимо установленного порядка с нарушением правил ее защиты. Несанкционированный доступ может осуществляться с помощью программных, аппаратных и иных средств, что свидетельствует о тесной взаимосвязи перечисленных выше групп способов. Например, несанкционированный доступ к компьютерной информации с помощью вредоносной программы класса троянов свидетельствует о комплексном использовании способов совершения преступлений.

В УК под *модификацией* согласно ст. 350 УК понимается «изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившее существенный вред, при отсутствии признаков преступления против собственности (модификация компьютерной информации)».

Модификации компьютерной информации, как правило, предшествует несанкционированный доступ к ней, что представляет практический интерес в плане обнаружения следов проникновения при выявлении признаков модификации компьютерной информации. При этом довольно простым способом в своем техническом исполнении является использование чужих сетевых реквизитов для доступа в сеть Интернет, при котором модификация происходит в автоматическом режиме. При доступе неправомерного пользователя с использованием чужих сетевых реквизитов в компьютерную сеть провайдера для последующего доступа в сеть Интернет в биллинговой системе (системе расчетов, позволяющей

в режиме реального времени производить необходимые расчеты объема услуг и денежных средств) провайдера происходят изменения компьютерной информации о времени правомерного пользования услугой и сумме, подлежащей к оплате. В то же время для неправомерного использования сетевых реквизитов необходимо получить доступ к ним, что нередко сопряжено с несанкционированным доступом при помощи вредоносных программ. Таким образом, получается цепочка из преступных действий, направленных на достижение общей противоправной цели.

Среди способов, направленных на *уничтожение (блокирование) информации* в компьютерной системе, сети или на машинном носителе или их самих, помимо уничтожения самой компьютерной информации следует рассматривать также уничтожение компьютерной системы, сети или машинного носителя, что означает полное или частичное их физическое уничтожение либо утрату их функциональных характеристик.

Блокирование компьютерной информации – искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением. Внешнее проявление блокирования, как правило, выражается в виде временной остановки работы компьютера («зависания»). Рассматриваемая группа способов наиболее опасна для работы компьютерной системы и сети ввиду уничтожения самих физических носителей информации, оборудования, что может повлечь тяжкие последствия и необратимую утрату ценных сведений.

При рассмотрении группы способов, направленных на *неправомерное завладение компьютерной информацией*, следует принять во внимание, что копирование компьютерной информации – повторение и устойчивое запечатление ее на машинном или ином носителе. При этом понятие «завладение» шире, чем понятие «копирование» и включает его. Следовательно, диспозиция ст. 352 УК охватывает также действия правонарушителя по завладению машинным носителем в виде накопителя на жестких магнитных дисках или иным носителем с охраняемой законом информацией, если в процессе расследования уголовного дела будет установлена и доказана направленность умысла преступника именно на завладение информацией независимо от ее носителя. Это обстоятельство необходимо учитывать в ходе расследования при отграничении данного криминального деяния от преступлений против собственности.

Неправомерному завладению компьютерной информацией, как правило, предшествует несанкционированный доступ к ней, и такие деяния образуют совокупность преступлений. Следовательно, при получении сведений о фактах неправомерного завладения компьютерной информацией проводится комплекс проверочных мероприятий, направленных на установление источника и способа ее получения. При наличии сведений о фактах несанк-

ционированного доступа к компьютерной информации предпринимаются попытки отыскать следы такого доступа в компьютерной системе.

Под *незаконным оборотом* понимаются изготовление (разработка, внесение изменений), распространение, использование или сбыт перечисленных выше средств и программ. При этом в соответствии с позицией законодателя, изложенной в УК, различаются программы, предназначенные для получения несанкционированного доступа к компьютерной информации, вредоносные и вирусные программы. Вышеуказанные программные средства могут сочетать свойства вирусных, вредоносных программ и программ для получения несанкционированного доступа.

Вредоносность или полезность для компьютера соответствующих программ определяется вне зависимости от их назначения, способности уничтожать, блокировать, модифицировать, копировать информацию (как правило, это вполне типичные функции обычных программ). Основным критерием отграничения будет следующее: предполагает ли их работа, во-первых, предварительное уведомление собственника компьютерной информации или другого добросовестного пользователя о характере действия программы и, во-вторых, получение его согласия (санкции) на реализацию программой своего назначения. Нарушение одного из этих требований делает программу вредоносной для компьютера, поскольку вредоносность так называемых компьютерных вирусов связана с их свойством самовоспроизводиться и создавать помехи в работе компьютера без ведома и санкции добросовестных пользователей.

Указанные положения имеют существенное значение при рассмотрении способов, связанных с незаконным оборотом программных или аппаратных средств, предназначенных для получения несанкционированного доступа к компьютерной информации, либо вредоносных программ.

При *расследовании преступлений, связанных с эксплуатацией компьютерной системы или сети*, основным обстоятельством, подлежащим доказыванию, выступает факт противоправного нарушения правил. При этом в настоящее время нормативно закрепленного определения таких правил нет. Это может вызвать противодействие следствию путем апеллирования обвиняемого (его защитника) к тому, что определенные действия правонарушителя не урегулированы какими-либо правилами либо регламентированы недостаточно.

Однако в общем виде правила эксплуатации компьютера определяются соответствующими техническими нормативными актами. Они также излагаются в паспортах качества, технических описаниях и инструкциях по эксплуатации, передаваемых пользователю при приобретении средств компьютерной техники (компьютера и периферийных устройств), правилах пользования компьютерными сетями, в инструкциях по использованию программ для компьютера как на бумажных, так и на машинных носителях информации. В последнем случае они включаются в программу, обеспечивающую к ним доступ при желании пользователя. Также к правилам эксплуатации компьютерной системы, сети можно отнести должностные инструкции лиц, имеющих доступ к данной системе или сети.

Комплексное использование представляет собой совокупность описанных выше *способов совершения в различной вариации* в зависимости от личности преступника, его целей и обстановки, в которой совершается преступление. Как правило, такие криминальные деяния представляют собой сложные, тщательно продуманные, изощренные действия, характеризующиеся подготовкой к совершению преступления, непосредственно самим его совершением, которое может представлять собой многоэпизодное событие, и сокрытием следов преступной деятельности.

При расследовании преступлений против информационной безопасности возможны три типичных следственных ситуации.

Следственная ситуация 1: ***имеются данные, указывающие на признаки преступления, сведения о лице (лицах), причастном к его совершению, отсутствуют***.

Источниками получения информации, содержащей данные, указывающие на признаки преступления, чаще всего выступают заявления граждан, сообщения должностных лиц организаций, которые, как правило, пострадали от совершенного противоправного деяния. При этом потерпевшая сторона обычно неохотно заявляет о совершенном в отношении ее преступлении. Это объясняется нежеланием предавать огласке собственные незаконные действия (например, наличие «двойной бухгалтерии» у субъекта хозяйствования) либо показывать некомпетентность своих работников, а также в ряде случаев невозможностью самостоятельного установления характера происшедшего события. В такой ситуации большое значение приобретает оперативная работа по выявлению признаков противоправных деяний.

Характер полученной информации относительно события преступления и лиц, его совершивших, не отличается большой информативностью и характеризуется, как правило, отсутствием сведений о личности преступника. При получении подобной информации следователь как можно быстрее прибывает на место происшествия для непосредственного изучения происшедшего события и тщательного исследования следов криминальной деятельности. Самостоятельный анализ обстановки совершения и объектов – носителей следовой информации позволяет предположительно установить способ совершения противоправного деяния. В свою очередь, совокупность полученной информации помогает выдвинуть версии относительно личности правонарушителя.

По прибытии на место происшествия следователь устанавливает, совершено ли преступление против информационной безопасности или иное противоправное деяние либо анализ первоначальных следственных

данных свидетельствует об отсутствии признаков криминального деяния. В любом случае важнейшей задачей на данном этапе является проведение полного и тщательного *осмотра места происшествия* с целью установления и фиксации следов противоправной деятельности, служащих основой для выдвижения версий. Соответственно, при установлении признаков совершения преступления в сфере информационной безопасности на основе первоначальных данных, полученных в ходе осмотра места происшествия, следователь выдвигает общие версии относительно происшедшего события: имело место преступление, предусмотренное гл. 31 УК; имело место преступление, предусмотренное иными главами УК; преступления не было, лицо, сообщившее о преступлении, добросовестно заблуждается относительно характера имевшего место события.

Обобщение сведений, полученных при опросе свидетелей, сопоставление их с информацией, полученной при исследовании объектов – носителей следов криминальной деятельности и обстановки реализации преступного замысла, позволяют выдвинуть частные версии, касающиеся, например, способа совершения преступления, личности преступника, предмета преступного посягательства и т. д. Кроме того, отнесение расследуемого криминального деяния к группе преступлений в сфере информационной безопасности позволяет использовать обобщенные данные криминалистической характеристики при выдвижении частных версий по отдельным ее элементам. В силу этого частные версии могут быть выдвинуты:

– относительно личности преступника;

– способа и мотивов совершения преступления;

– предмета криминального посягательства;

– обстоятельств совершения преступления;

– места совершения противоправного деяния (с учетом специфики, рассмотренной выше) и т. д.

Например, в ходе предварительного осмотра компьютерной техники обнаружена вредоносная программа. В этой ситуации устанавливается давность заражения ею компьютерной системы путем проверки в свойствах программы времени ее создания (изменения) и сравнения его с системным временем компьютерной системы. В ходе допросов собственников (пользователей) устанавливается, изменялось ли ими системное время, когда и по какой причине, кто имел доступ к компьютерной системе, подключена ли она к локальной или глобальной компьютерной сети, установлена ли система защиты, каков принцип ее действия и т. д. Выяснение этих временных показателей и иных обстоятельств оказывает значительное влияние на процесс выдвижения версий и позволяет существенно сузить круг подозреваемых лиц.

Следующим шагом следователя на пути к установлению истины по делу закономерно выступает *определение направлений расследования*

в ситуации, которую можно охарактеризовать как информационно неопределенную. В этом случае основными направлениями расследования будут являться следующие:

– получение в ходе первоначальных следственных действий сведений, характеризующих личность преступника, места его возможного нахождения;

– выявление отличительных признаков способа противоправного посягательства, в том числе указывающих на конкретное лицо;

– определение круга подозреваемых лиц и проверка их причастности к совершенному преступлению;

– установление полной картины совершенного преступления с целью выявления мотивов его совершения и иных обстоятельств, имеющих первостепенное значение для идентификации преступника.

Проблемы с поводами к возбуждению уголовного дела в этой следственной ситуации, как правило, не возникают. Сложнее обстоит ситуация с *установлением оснований к возбуждению уголовного дела*. Так, ст. 167 УПК устанавливает, что основаниями к возбуждению уголовного дела являются: наличие достаточных данных, указывающих на признаки преступления, при отсутствии обстоятельств, исключающих производство по уголовному делу.

При получении первичных сведений в ряде случаев возникают вопросы, связанные с установлением достаточных данных, указывающих на признаки преступления. Это обстоятельство обусловливает необходимость проведения доследственной проверки с целью установления необходимых для возбуждения уголовного дела сведений. По следственным ситуациям, связанным с незаконным оборотом программных или аппаратных средств, предназначенных для получения несанкционированного доступа к компьютерной информации, либо иных вредоносных программ, проведение подобной проверки практически всегда обязательно с целью установления в ходе проведения компьютерно-технической экспертизы оснований к возбуждению уголовного дела. Такими основаниями в данном случае будут установленные в ходе экспертизы вредоносные свойства программных средств или выводы эксперта о наличии в программных или аппаратных средствах функций для получения несанкционированного доступа к компьютерной информации.

Перечень *обстоятельств, подлежащих доказыванию* при расследовании преступления в данной следственной ситуации, довольно обширен:

– имело ли место событие преступления либо иное правонарушение (устанавливается факт, место и время совершения преступления в сфере информационной безопасности);

– что является объектом преступного посягательства (установление факта противоправного посягательства на отношения по поводу использования компьютерной информации является принципиально важным для отграничения преступлений в сфере информационной безопасности от смежных составов и применения соответствующей методики их расследования);

– какой способ совершения преступления в этой сфере использовался преступником (устанавливаются способ совершения преступления, метод и период времени для преодоления средств защиты информации, использованные для этого аппаратные и программные средства);

– что являлось предметом преступного посягательства (на что были направлены действия преступника (установление такого обстоятельства позволит определить мотив и цель совершения преступления), например, предметом преступного посягательства явилась база данных провайдера услуг сети Интернет, которая находилась на машинных носителях компьютера, не подключенного к глобальной информационной сети, следовательно, можно предположить, что криминальное деяние совершено работником этой организации с корыстными целями или по мотивам мести);

– каковы характер и размер вреда, причиненного в результате противоправного деяния (установление этих обстоятельств представляет собой довольно нелегкую задачу, так как вред редко выражается в виде прямых убытков. Например, широко известные вирусные атаки приносят вред в виде затрат на обнаружение вирусной программы и ее нейтрализацию, при этом во вред включается сумма оплаты специалистам времени, затраченного на устранение вирусной программы, вынужденного простоя компьютерных систем и т. д.);

– какова степень виновности лица в совершении преступления (в случае совершения криминального деяния группой лиц устанавливаются участники, их роль и степень участия). Сложные многоэпизодные преступления совершаются, как правило, группой лиц, поэтому в ходе допросов тщательно выясняются соучастники криминального деяния. Это обусловлено тем, что при совершении сложного высокотехнологичного преступления необходимы хорошие знания в нескольких сферах использования компьютерных технологий, что предполагает привлечение соучастников в качестве соисполнителей либо пособников, оказывающих консультационную помощь;

– какие обстоятельства влияют на степень и характер ответственности обвиняемого (смягчающие и отягчающие ответственность, характеризующие личность обвиняемого)?

На первоначальном этапе расследования в число *неотложных следственных действий и иных мероприятий* целесообразно включить:

– осмотр места происшествия;

– допрос свидетелей, потерпевших с целью получения информации, которая может способствовать установлению преступника и иных обстоятельств, имеющих значение для дела;

– направление сотрудникам оперативных подразделений отдельных поручений на проведение оперативно-розыскных и иных мероприятий с целью установления личности преступника, его местонахождения и последующего задержания (в основу розыскных мероприятий может быть положена информация, полученная в ходе допроса свидетелей, исследования места происшествия, а также данные криминалистической структуры, позволяющие на основе известной информации о ее некоторых элементах выдвинуть версии относительно иных, неизвестных элементов);

– выемку предметов и документов (с учетом специфики следственной ситуации);

– осмотр помещений, жилища и иного законного владения, не являющихся местом происшествия (для установления дополнительных следов преступной деятельности);

– назначение компьютерно-технических и иных экспертиз в зависимости от обнаруженных объектов – носителей следов криминальной деятельности;

– иные следственные действия и оперативно-розыскные мероприятия, направленные на установление и доказывание обстоятельств совершенного преступления.

Следственная ситуация 2: ***имеются данные, указывающие на признаки преступления, сведения о лице (лицах), причастном к его совершению, неполные либо неточные***.

Особенностью данной следственной ситуации является то, что она характерна для совершения преступлений в организациях и источниками получения сведений о совершенном преступлении, как правило, выступают сообщения должностных лиц организации и непосредственное обнаружение сотрудниками правоохранительных органов признаков противоправного деяния в результате проведенной оперативной работы. В случае поступления сообщений о криминальных деяниях от работников организации наиболее вероятной будет версия о совершении преступления лицом, состоящим в трудовых отношениях с этой организацией. Однако в настоящее время этот повод к возбуждению уголовного дела не характерен для Республики Беларусь. При этом сообщения в электронных средствах массовой информации, на интернет-форумах могут являться поводами к возбуждению уголовного дела лишь при со-

блюдении условий, предусмотренных ст. 171 УПК, в остальных случаях такие сведения имеют оперативно-розыскной характер.

Основным направлением расследования будет *установление полных данных предполагаемого преступника, места его нахождения и последующее задержание*. Такие сведения могут быть получены в ходе допроса заявителей, работников организации, где совершено преступление, и иных лиц, могущих охарактеризовать преступника, а также лиц, ответственных за защиту информации. Параллельно установлению правонарушителя осуществляется *фиксация доказательственной информации*, позволяющая впоследствии изобличить предполагаемого правонарушителя. Фиксация производится путем проведения осмотра места происшествия, предварительного исследования и последующего изъятия компьютерной техники, получения необходимых сведений у предприятий связи, предоставляющих доступ в сеть Интернет, обысков на рабочих местах и по месту жительства подозреваемых лиц, выемки документации, регламентирующей производственный процесс, в ходе которого было совершено преступление, документов, определяющих перечень трудовых обязанностей персонала, в том числе и предполагаемого правонарушителя.

После закрепления доказательственной информации и установления сведений о личности предполагаемого преступника проводится комплекс следственных действий, оперативно-розыскных мероприятий, направленных на проверку причастности данного лица к совершенному преступлению. К таким действиям относится допрос подозреваемого лица, в ходе которого выясняется причастность к противоправному деянию; его роль в случае, если преступление совершено в группе; наличие пособников и т. д. При необходимости проводится очная ставка между подозреваемым и иными лицами с учетом материалов дела. Кроме того, осуществляется комплекс оперативно-розыскных мероприятий, направленных па проверку причастности подозреваемого к расследуемому и иным преступлениям, обнаружение мест возможного нахождения следов криминального деяния и лиц, могущих быть свидетелями по делу (например, путем проведения аналитической разведки в сети Интернет).

Круг и характер общих и частных версий в целом совпадают с вариантом, рассмотренным по первой следственной ситуации. Однако имеющаяся информация о подозреваемом может быть умышленно искажена с целью введения следствия в заблуждение, поэтому первостепенное значение в рассматриваемой следственной ситуации приобретает фиксация следов преступной деятельности.

Данные, свидетельствующие о совершении преступления против информационной безопасности, могут быть получены в ходе проведения следующих *следственных действий и иных мероприятий*:

– допроса свидетелей, потерпевших с целью установления сведений, позволяющих определить данные о предполагаемом преступнике и его причастности к совершению преступления;

– опроса до начала осуществления осмотра места происшествия, позволяющего целенаправленно изучать следы противоправной деятельности;

– осмотра места происшествия с изъятием компьютерной техники, ставшей средством совершения преступления или предметом противоправного посягательства;

– выемки и осмотра документации, регламентирующей производственный процесс, обязанности персонала;

– обысков на рабочем месте и по месту жительства предполагаемого преступника;

– направления поручений сотрудникам оперативных подразделений на проведение оперативно-розыскных и иных мероприятий с целью установления причастности лица к совершению расследуемого и иных преступлений;

– назначения компьютерно-технических и других экспертиз;

– иных следственных действий и оперативно-розыскных мероприятий с учетом обстоятельств дела.

Следственная ситуация 3: ***имеются данные, указывающие на признаки преступления, при этом установлено лицо, его совершившее, и его местонахождение***.

Информация о преступлении в данной следственной ситуации может быть получена от граждан (собственников и законных владельцев компьютерной техники), которые пострадали от совершенного противоправного деяния, а также путем непосредственного обнаружения признаков преступления органами уголовного преследования в ходе проверки сообщений, поступивших из оперативных источников, о готовящемся или совершенном противоправном деянии, при проведении специальных технических мероприятий, задержании лица на месте совершения криминального деяния.

В то же время для данной группы преступлений не характерно получение сведений о совершенном преступлении от правонарушителей в виде явки с повинной.

С учетом ранее приведенных рекомендаций в данной следственной ситуации необходимо провести следующие *следственные действия и иные мероприятия*:

– решить вопрос о возможности задержания преступника с поличным и о необходимых в связи с этим мероприятиях;

– провести осмотр места происшествия с участием заранее приглашенных специалистов;

– провести личный обыск подозреваемого, а также обыски по месту работы и месту жительства (с учетом тактических особенностей их осуществления);

– допросить подозреваемого об обстоятельствах противоправного деяния;

– направить поручение в оперативное подразделение по установлению причастности подозреваемого к иным преступлениям, его связей и иных лиц, которые могут быть соучастниками совершения криминального деяния;

– допросить свидетелей (очевидцев) об участии правонарушителя и его роли в совершении преступления;

– провести выемку и осмотр предметов, документов (в том числе и на машинных носителях), отражающих протоколирование работы пользователей, признать их вещественными доказательствами;

– истребовать, а при необходимости провести выемку нормативных актов и документов, характеризующих порядок и организацию работы с конфиденциальной информацией, компьютерной информацией, ЭВМ, компьютерной сетью;

– решить вопрос о необходимости назначения экспертиз, проведения проверок финансово-хозяйственной деятельности.

Особенности назначения компьютерно-технических экспертиз.

Компьютерно-техническая экспертиза – самостоятельный род судебных экспертиз, относящийся к классу технических.

Компьютерно-техническая экспертиза проводится в целях: определения статуса объекта как компьютерного средства, выявления и изучения его роли в расследуемом преступлении, а также получения доступа к информации на носителях данных с последующим всесторонним ее исследованием.

При проведении компьютерно-технической экспертизы решаются в основном следующие *задачи*:

– определение вида (типа, марки), свойств аппаратного средства, а также его технических и функциональных характеристик;

– определение фактического состояния и исправности аппаратного средства, наличия физических дефектов;

– определение основных характеристик операционной системы;

– выявление и исследование функциональных свойств, а также настроек программного обеспечения, времени его инсталляции;

– определение фактического состояния программного объекта, состава соответствующих ему файлов, их параметров (объемы, даты создания, атрибуты), способов ввода-вывода информации, наличия или

отсутствия каких-либо отклонений от типовых параметров (например, недокументированных функций);

– диагностирование алгоритма программного продукта, видов использованных при его разработке инструментальных средств;

– установление первоначального состояния программы (например, при начальной инсталляции) и выявление возможных последующих изменений;

– выявление структуры механизма события по результатам работы программного обеспечения и в динамике;

– установление причинной связи между действиями пользователя компьютерной системы в отношении программного обеспечения и наступившими последствиями;

– идентификационные задачи, связанные с индивидуальным отождествлением оригинала программы (инсталляционной версии) и ее копии на носителях данных компьютерной системы;

– отождествление содержания файла с данными в копии исследуемого файла либо в представленном документе (в том числе в бумажной копии в комплексе с технической экспертизой документов).

Кроме того, в ходе проведения компьютерно-технической экспертизы решаются следующие задачи.

1. *Поиск на компьютерном носителе документов*, изображений, сообщений и иной информации, относящейся к делу, в том числе в неявном (удаленном, скрытом, зашифрованном) виде.

В связи с большим объемом информации, как правило, невозможно распечатать и приложить к заключению все имеющиеся на носителе текстовые и графические файлы, содержимое баз данных с тем, чтобы потом следователь решил, что из найденного относится к делу. Эксперт в любом случае вынужден проводить первичную селекцию и принимать решение, что именно из найденного приобщать, поэтому эксперта следует ознакомить с уголовным делом или хотя бы кратко изложить его фабулу в постановлении о назначении компьютерно-технической экспертизы. Необходимо определять критерии поиска – ключевые слова или ограничивать рамки поиска типом файлов (например, следствие интересуют графические файлы с изображением бланков документов, печатей и штампов, текстовые файлы или электронные таблицы и т. д.).

Поиск «цифровых» следов различного рода действий, совершаемых с компьютерной информацией. Когда компьютер используется как средство доступа к информации, находящейся в ином месте, и когда доступ к информации осуществляется на этом компьютере – в обоих случаях остаются «цифровые» следы, следы в виде компьютерной информации. Компьютерно-техническая экспертиза может определить, когда, при ка-

ких условиях и каким образом осуществлялся доступ. Кто его осуществлял, компьютерно-техническая экспертиза определить не может. Лишь в некоторых случаях эксперту удается обнаружить некоторые сведения о пользователе исследуемого компьютера.

Действия, которые оставляют следы на компьютере или на носителе информации, включают: доступ к информации, ее просмотр, ввод, изменение, удаление, любую другую обработку или хранение, а также удаленное управление этими процессами.

2. *Анализ компьютерных программ* проводится для с целью определения их функциональности и следов их использования, принципа действия, вероятного их источника, происхождения, сведений об авторе, наличия вредоносных признаков, их принадлежности к средствам преодоления технических средств защиты авторского права и т. д.

Часто при этом необходимо более глубокое исследование программ, т. е. исследование не просто их свойств и функциональности, а происхождения, особенностей взаимодействия с другими программами, процесса создания, сопоставление версий. Такое глубокое исследование подразумевает дизассемблирование программы, запуск под отладчиком (пошаговое исполнение), исследование структуры данных. В таком случае рекомендуется назначать две отдельные экспертизы: первая изучает содержимое компьютерных носителей, а вторая – особенности обнаруженных программ.

Установление времени и последовательности совершения пользователем различных действий. Благодаря наличию у компьютера внутренних энергонезависимых часов и простановке в различных местах временных меток становится возможным определить, когда и в какой последовательности пользователь производил различные действия.

Если внутренние часы компьютера были переведены вперед или назад (в том числе неоднократно), все равно имеются возможности восстановить правильное время и правильную последовательность событий. Перевод часов компьютера сам по себе оставляет следы. Если было сетевое взаимодействие, существует возможность сопоставить моменты событий, зафиксированных данным компьютером, с событиями по иным источникам и выяснить сдвиг внутренних часов.

Задача выполнима даже в том случае, если системный блок, содержащий внутренние часы, не находится в распоряжении экспертизы. Только по носителю информации можно получить кое-какие сведения о последовательности событий. Чем больше информации на носителе, тем полнее будет восстановлена картина.

Решая вопрос о назначении экспертизы, следователь должен акцентировать внимание на поиске, фиксации, изъятии и представлении эксперту необходимых материальных объектов – носителей информации, а также

на уяснении и формировании задач, стоящих перед следствием. Постановка излишне общих вопросов, не имеющих значения для рассматриваемого дела, является наиболее типичной ошибкой при назначении компьютерно-технической экспертизы. Примеры ошибочных вопросов: каково содержание удаленной информации; имеются ли на накопителе базы данных, если да, то какая информация в них содержится; какая информация содержится на накопителе на жестких магнитных дисках?

Примерные вопросы, решаемые компьютерно-технической экспертизой:

– соответствует ли комплектация представленных на исследование системных блоков комплектации, указанной в гарантийных талонах на них;

– имеются ли на носителе представленного на исследование системного блока персонального компьютера файлы, в том числе удаленные, содержащие информацию о... (следует указать конкретные ключевые слова для поиска – названия организаций, фамилии и т. д.);

– имеются ли на носителе представленного на исследование системного блока персонального компьютера графические файлы, в том числе удаленные, содержащие изображения денежных билетов, купюр, и т. д.;

– имеется ли на накопителе на жестких магнитных дисках представленного на исследование системного блока информация о реквизитах для доступа в сеть Интернет;

– имеются ли на носителе представленного на исследование системного блока компьютера журналы работы программ, предназначенных для просмотра сайтов сети Интернет; если да, то ссылки на какие сайты сети Интернет в них имеются;

– какие функции реализует программа, имеющаяся на представленном на исследование компакт-диске, и какие действия она выполняет в случае ее запуска на компьютере;

– имеются ли на носителях информации, представленных на исследование системных блоков компьютера, журналы работы программ обмена сообщениями в сети Интернет; если да, то какие сообщения в них содержатся?

Эксперт не может определить правомерность доступа, осуществлявшегося с исследуемого компьютера или на исследуемый компьютер. Таким образом, вопрос «Имеются ли на носителях информации программы, предназначенные для осуществления несанкционированного доступа к информации, хранящейся в компьютерной системе, сети или на машинных носителях?» является недопустимым. Правомерность, как и контрафактность, факт юридический, а не технический.

Также в случае вредоносности. Вредоносность – правовое понятие, которое устанавливается судом по результатам экспертиз и обстоятельств дела, но не экспертом.

Например, программа для негласного собирания информации в локальной сети организации может легально использоваться администратором для слежения за компьютерами пользователей по правилам внутреннего распорядка, которые юридически закреплены в нормативных документах этой организации. Не в компетенции эксперта, проводящего компьютерно-техническую экспертизу, разбираться с юридическими тонкостями использования таких программных продуктов. Эксперт, проводящий компьютерно-техническую экспертизу, может описать условия работы данного программного обеспечения на компьютере и установить его функциональность. Поэтому вопрос «Является ли программа… вредоносной?» также является недопустимым.

Эксперт может определить ряд других фактов, которые позволят следствию и суду квалифицировать доступ как правомерный или неправомерный либо отнести программный продукт к вредоносным. Это следующие факты:

– к какой именно информации осуществлялся доступ (для последующего решения вопроса, является ли она охраняемой законом компьютерной информацией);

– предпринимал ли обладатель информации, к которой был осуществлен доступ, какие-либо меры для ее защиты и ограничения доступа (для решения вопроса о конфиденциальности этой информации);

– является ли данный способ доступа общепринятым способом для публичных сетевых ресурсов;

– условия установки, работы программы, ее функциональность и следы ее использования?

При постановке вопроса необходимо использовать устоявшийся понятийный аппарат, исключающий жаргонные и полупрофессиональные термины (винчестер, логи, взлом и т. д.). В случае отсутствия терминов, определенных законодательными или нормативными актами, необходимо использовать те термины, которые употребляют разработчики технических средств, программных продуктов в документации, описаниях, справках и т. д. Вопрос должен быть четким и однозначным. Формулировка вопроса не должна касаться этапов исследования информации (описание характеристик носителей информации и особенностей размещения информации на них, восстановление и исследование информации среди удаленных файлов являются обязательным этапом исследования информации). Вопросы не должны носить справочный характер. Вопросы не должны носить правовой характер и выходить за пределы компетенции эксперта. Вопросы должны соответствовать существующей методической и технической базе.

8. СОВРЕМЕННЫЕ МЕТОДЫ И СРЕДСТВА СОВЕРШЕНСТВОВАНИЯ ОРГАНИЗАЦИИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

В настоящее время остро стоит вопрос совершенствования не только методики расследования преступлений в сфере высоких технологий, но и тактики проведения отдельных следственных действий. Некоторые аспекты внедрения высоких технологий в деятельность следователя коснулись такого следственного действия, как допрос.

Под *допросом* понимают следственное действие, заключающееся в получении следователем, лицом, производящим дознание, в устной или письменной форме показаний об обстоятельствах, имеющих значение для дела, от свидетеля, потерпевшего, подозреваемого, обвиняемого. Допрос является самым распространенным следственным действием. Нет ни одного уголовного дела, которое могло быть законченным без допросов. А в отдельных случаях проведение данного следственного действия является обязательным.

Как правило, допрос проводится по месту проведения предварительного расследования. Вместе с тем в соответствии с ч. 1 ст. 215 УПК «следователь, лицо, производящее дознание, вправе, если признают это необходимым, провести допрос по месту нахождения допрашиваемого».

Сегодня по-прежнему актуальным остается вопрос: как быть, если возникает необходимость допросить участника уголовного процесса, находящегося в другой местности? В настоящее время существуют три варианта развития событий по предложенному сценарию:

1) направление поручения (ходатайства) о проведении следственных действий в порядке ч. 4 ст. 184 УПК, которая гласит: «В случае необходимости производства следственных действий в другой местности следователь, орган дознания вправе произвести их лично либо поручить производство этих действий следователю, органу дознания по территориальности. <…> Поручение дается в письменной форме и подлежит выполнению в срок не позднее десяти суток…»;

2) вызов участника повесткой к месту производства предварительного расследования;

3) выезд следователя, лица, производящего дознание, в командировку.

Наиболее распространенным вариантом из перечисленных является первый. Вместе с тем далеко не всегда следователи остаются удовлетворены эффективностью исполнения таких поручений. Это касается не только сроков их исполнения, но и качества проведения рассматриваемого следственного действия. Допрос желательно проводить самому. Постороннее лицо, не владеющее материалами уголовного дела, вряд ли сможет выяснить абсолютно все вопросы, стоящие перед следствием. Не решают данную проблему и методические рекомендации о необходимости указания в поручении перечня вопросов, на которые следует получить ответ (ведь в ходе получения показаний допрашиваемого могут появиться новые факты, требующие незамедлительного выяснения, на которые сможет обратить внимание лишь должностное лицо, досконально знающее материалы конкретного уголовного дела).

Реже практикуется вызов участника к месту производства предварительного расследования. Данный способ является наиболее эффективным с содержательной точки зрения, хотя при этом весьма сложен в организационном аспекте: вызвать лицо из другой области, при необходимости помочь ему с проживанием, наконец, своевременно решить вопрос об оплате последнему понесенных расходов. В соответствии с п. 1–3 ч. 1 ст. 162 УПК процессуальные издержки складываются в том числе:

– из сумм, выплачиваемых потерпевшим, свидетелям на покрытие их расходов по явке к месту проведения процессуального действия и обратно, по найму жилого помещения, а также в качестве суточных;

– сумм, выплачиваемых потерпевшим, свидетелям, не имеющим постоянного заработка, за отвлечение их от обычных занятий;

– сумм, выплачиваемых потерпевшим, свидетелям, работающим и имеющим постоянный заработок, в возмещение недополученной ими заработной платы за все время, затраченное в связи с вызовом в орган, ведущий уголовный процесс.

Данные обстоятельства не только усложняют, но и удорожают уголовный процесс.

Направление сотрудников в командировки в организационном аспекте также является довольно сложным и дорогостоящим процессом.

Все вышеуказанное обретает еще большую актуальность в том случае, если потерпевший, свидетель проживают за пределами Республики Беларусь. При этом существенно увеличивается срок исполнения поручения, остается меньше возможностей для дополнительного или повторного допроса в случае некачественного его проведения, повышается сложность обеспечения вызова лица на территорию Республики Беларусь для проведения допроса, существенно увеличиваются процессуальные издержки, вопрос о командировке решается лишь в исключительных случаях руководством ведомства и т. д.

Следователи, будучи осведомленными о таких сложностях, в отдельных случаях изобретают новые возможности «получения показаний на расстоянии».

В практической деятельности органов уголовного преследования встречаются и случаи упрощенческого подхода к производству допроса участника уголовного процесса, находящегося в другой местности. В данном случае речь идет о так называемых справках, составляемых должностными лицами органа уголовного преследования, когда следователь, будучи ограниченным истекающими сроками расследования, так и не дождавшись ответа на направленное поручение о производстве допроса (а иногда и не направляя таковое), сам по телефону связывается со свидетелем, выясняет интересующую его информацию и помещает в материалы уголовного дела справку примерно следующего содержания: «Сообщаю, что я по телефону номер… связался с гр-ном… являющимся свидетелем по настоящему уголовному делу, который в телефонной беседе сообщил следующее... (фактически расписываются показания такого участника)». Естественно, что такие «допросы» не имеют абсолютно никакой юридической силы и являются недопустимыми.

В контексте затронутой проблемы возникает закономерный вопрос: имеются ли дополнительные неисследованные возможности порядка проведения допроса лиц, находящихся в другой местности, с целью ускорения и удешевления процедуры его производства в строгом соответствии с положениями УПК? Ответить на него следует положительно.

Научно-технический прогресс не стоит на месте. То, что несколько лет назад считалось чем-то удивительным, сегодня является обыденностью жизни. Сегодня не является необычным факт подписания организациями контрактов по факсу, проведение видеоконференций, в том числе посредством Skype – программы, имеющейся у большинства пользователей сети Интернет. К данным средствам могут обратиться и должностные лица органа уголовного преследования.

Порядок проведения *допроса через сеть Интернет* следующий: в каждом подразделении органа, ведущего уголовный процесс, имеется доступ к сети Интернет. Для целей проведения допроса необходимо выделить один компьютер с доступом к сети Интернет, установленной программой Skype, с поддержкой видеозвонков и обязательным наличием web-камеры. При необходимости производства допроса участника,

находящегося в другой местности, следователь, лицо, производящее дознание, вызывают такого участника в ближайший к месту жительства последнего орган уголовного преследования, где должностное лицо отдела режимно-секретной деятельности, группы защиты информации, следователь, лицо, производящее дознание, оперативный дежурный оперативно-дежурной службы (применительно к органам внутренних дел) или любое другое должностное лицо, имеющее право пользования выделенным компьютером, приглашает вызванного участника в соответствующее помещение и в режиме видеозвонка связывается с инициатором допроса. После установления видеосвязи следователь, лицо, производящее дознание, приступают к проведению допроса.

С этого момента каждое действие должностного лица, ведущего уголовный процесс, должно соответствовать требованиям уголовно-процессуального закона, в первую очередь ст. 217 «Общие правила проведения допроса», ст. 218 «Протокол допроса» и ст. 219 «Применение звуко- и видеозаписи при допросе» УПК.

В соответствии с ч. 1 ст. 217 УПК перед допросом следует выяснить данные о личности допрашиваемого. Этот факт может быть зафиксирован двумя способами: 1) допрашиваемое лицо крупным планом показывает документ, удостоверяющий личность, в целях получения четкого изображения на компьютере следователя; 2) должностное лицо органа уголовного преследования, присутствующее при допросе в одном месте с допрашиваемым, сверяет с документами сообщенные допрашиваемым сведения.

В соответствии с ч. 2 ст. 217 УПК лицу, вызванному на допрос, сообщается, в качестве кого, по какому уголовному делу оно будет допрошено, разъясняются права и обязанности, предусмотренные ст. 41, 43, 50 и 60 УПК, в том числе право отказаться от дачи показаний в отношении его самого, членов его семьи и близких родственников, о чем делается отметка в протоколе. Лицо, вызванное на допрос в качестве потерпевшего или свидетеля, предупреждается об уголовной ответственности за отказ или уклонение от дачи показаний и за дачу заведомо ложных показаний. В строгом соответствии с приведенными положениями должны быть сделаны и соответствующие разъяснения.

После завершения свободного рассказа и при необходимости получения ответов на дополнительные вопросы должностному лицу органа уголовного преследования следует приступить к оформлению протокола допроса.

В протоколе допроса должны быть отражены сведения о проведении допроса посредством технических средств связи (с указанием системного оборудования, программного обеспечения). Также необходимо указать на участие в допросе специалиста (при необходимости), а также

должностного лица органа дознания, присутствовавшего при допросе в одном помещении с допрашиваемым.

В соответствии с ч. 5 ст. 218 УПК по окончании допроса протокол предъявляется для прочтения допрашиваемому либо оглашается по его просьбе. При предлагаемом порядке производства данного следственного действия простое оглашение протокола может вызвать сомнения у суда в его объективности, поэтому более правильным видится незамедлительная передача протокола через сеть допрашиваемому для ознакомления.

Последующее распечатывание протокола допроса осуществляется следователем по месту своего нахождения. При этом к протоколу допроса прилагается запись всей видеоконференции. Несомненно, проблемным вопросом в данном случае является необходимость соблюдения положений ч. 4 ст. 219 УПК, в соответствии с которой по окончании допроса видеозапись полностью воспроизводится допрашиваемому, хотя и это технически осуществимо без каких-либо дополнительных затрат.

Еще одним вопросом, требующим детального изучения, должен быть вопрос об удостоверении факта ознакомления с показаниями и правильности их записи (ч. 6 ст. 218 УПК). Правила ст. 194 «Удостоверение факта отказа от подписания или невозможности подписания протокола следственного действия» УПК ввиду специфики причин, по которым допрашиваемый не может собственноручно подписать протокол, в данном случае неприменимы. Здесь имеются несколько возможностей соблюдения данной процедуры:

– в распечатанном протоколе допроса следователь делает отметку о невозможности подписать протокол ввиду объективных причин. При этом гарантом правильности записанных показаний будет выступать должностное лицо органа уголовного преследования, находившееся в одном помещении с допрашиваемым;

– протокол допроса распечатывается по месту нахождения допрашиваемого, где правильность записанных показаний удостоверяется подписью допрашиваемого и должностного лица органа уголовного преследования, присутствовавшего при этом. Затем протокол допроса в отсканированном виде направляется следователю, который ставит свою подпись, либо направляется следователю по факсу для исключения возможности внести дополнения, либо направляется следователю через секретариат посредством почты (в данном случае актуальным становится вопрос о времени на ожидание данного допроса);

– помимо указанного можно использовать и возможности, предоставленные Законом Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи».

Будут ли полученные таким образом доказательства отвечать критериям допустимости? Отвечая на данные вопросы, следует прибегнуть к фундаментальным положениям теории уголовного процесса об общих правилах проведения следственных действий, а также порядку проведения допроса (табл. 3).

Таблица 3

Соответствие порядка допроса посредством Skype общим правилам следственных действий

Общие правила следственных действий	Соответствие им порядка допроса посредством Skype
Проведение следственных действий должностным лицом, осуществляющим производство по уголовному делу	Допрос осуществляет следователь, в чьем производстве находится уголовное дело
Запрет на производство следственных действий в ночное время, за исключением случаев, не терпящих отлагательства	При указанных обстоятельствах данный запрет действует неукоснительно
Проведение следственных действий после возбуждения уголовного дела	Правило соблюдается неукоснительно
Разъяснение следователем (лицом, производящим дознание) лицам, привлеченным к участию в следственном действии, прав и обязанностей, а также порядка проведения следственного действия	Правило соблюдается неукоснительно
Применение технических средств и использование научно обоснованных способов обнаружения, фиксации и изъятия следов преступления и вещественных доказательств	В данном случае фиксация показаний осуществляется с применением технических средств
Возможность привлечения к участию в следственных действиях сотрудника органа дознания	Такая возможность присутствует
Продолжительность следственного действия в законе не установлена (исключением из общего правила является продолжительность допроса – ч. 2 ст. 215, ч. 1 ст. 434 УПК)	Правило соблюдается неукоснительно
Составление протокола следственного действия в ходе проведения данного действия или непосредственно после его окончания	Правило соблюдается неукоснительно

При этом нарушений уголовно-процессуального законодательства нет.

Рассмотренные возможности применимы и к другим следственным действиям, например: к предъявлению для опознания, в отдельных случаях к очной ставке и даже проверке показаний на месте (хотя в данном случае требования к техническому обеспечению будут несоизмеримо выше).

Также на первый взгляд может показаться, что указанный порядок возможен лишь при допросах потерпевших и свидетелей. Подозреваемых и обвиняемых же в силу их статуса допрашивать таким образом не следует. Однако и данных участников в отдельных случаях можно допросить через сеть Интернет (например, когда в отношении обвиняемого применена мера пресечения в виде заключения под стражу, последний находится в следственном изоляторе другого города, а следователю необходимо в ходе дополнительного допроса выяснить лишь несколько вопросов).

Помимо указанного есть и иные возможности, предоставляемые сетью Интернет. Так, в практике встречаются единичные случаи *получения информации у очевидцев преступления посредством интернет-переписки*. Действуют они лишь в тех случаях, когда имеется необходимость получения показаний у лица, проживающего в стране дальнего зарубежья. Указанные лица собственноручно записывают свои показания посредством компьютера и направляют их на электронный адрес (mail.ru, tut.by, yandex.ru и т. д.) следователю. Последнему остается лишь распечатать полученные сведения и приобщить к материалам уголовного дела посредством составления протокола осмотра (объектом осмотра в данном случае является страница интернет-сайта, накопитель на жестких магнитных дисках служебного компьютера, на котором сохранена данная информация).

Следует изучить и возможность *фиксации сведений посредством интернет-переписки в режиме on-line* в чатах. Данное действие может быть оформлено, например, следующим образом: составляется справка о переписке; осуществляется осмотр накопителя на жестких магнитных дисках служебного компьютера; текст переписки распечатывается и приобщается к протоколу осмотра.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Боровик, П.Л. Детская порнография: выявление и возбуждение уголовных дел : монография / П.Л. Боровик, Г.В. Федоров ; под ред. В.П. Шиенка. – М. : Юрлитинформ, 2013. – 248 с.

Вехов, В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники : учеб.-метод. пособие / В.Б. Вехов. – Изд. 2-е, доп. и испр. – М. : ЦИиНМОКП МВД России, 2000. – 64 с.

Гридюшко, П.В. Методика расследования уголовных дел о распространении порнографических материалов с использованием компьютерной техники в сети Интернет, локальных сетях : пособие / П.В. Гридюшко, И.Г. Мухин ; учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь». – Минск : Акад. МВД, 2014. – 41 с.

Козлов, В.Е. Теория и практика борьбы с компьютерной преступностью / В.Е. Козлов. – М. : Горячая линия – Телеком, 2002. – 336 с.

Лепехин, А.Н. Расследование преступлений против информационной безопасности: теоретико-правовые и прикладные аспекты : монография / А.Н. Лепехин. – Минск : Тесей, 2008. – 173 с.

Лившиц, Ф.Н. Оценка доказательств при расследовании преступлений, предусмотренных статьями 352–354 УК Республики Беларусь / Ф.Н. Лившиц // Бюл. гл. упр. предвар. расследования МВД Респ. Беларусь. – 2006. – № 25–26. – С. 357–372.

Степанов, В.В. Поисково-познавательная деятельность при расследовании преступлений, совершенных с использованием высоких технологий : монография / В.В. Степанов, М.А. Бабакова. – М. : Юрлитинформ, 2014. – 256 с.

Юбко, Ю.М. Особенности расследования уголовных дел о преступлениях против интеллектуальной собственности, когда объектом преступного посягательства является программный продукт : пособие / Ю.М. Юбко, И.А. Судникович ; учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь». – Минск : Акад. МВД, 2014. – 27 с.

ОГЛАВЛЕНИЕ

Учебное издание

ГРИДЮШКО Павел Владимирович
ЛЕПЁХИН Александр Николаевич
МУХИН Илья Геннадьевич и др.

ОРГАНИЗАЦИЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Учебное пособие

Редактор *М.Н. Колотуха*
Технический редактор *Ю.С. Романюк*
Корректор *А.С. Мигно*

Подписано в печать 29.03.2017. Формат 60×84 $^{1}/_{16}$.
Бумага офсетная. Ризография. Усл. печ. л. 8,14. Уч.-изд. л. 8,06.
Тираж 210 экз. Заказ 66.

Издатель и полиграфическое исполнение:
учреждение образования
«Академия Министерства внутренних дел Республики Беларусь».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий № 1/102 от 02.12.2013.
Пр-т Машерова, 6, 220005, Минск.