кругу. Получив данные о таком количестве лиц, представители органов расследования теряются и попросту отказываются от проверки поступившей информации либо пытаются проверять ее выборочно. В последнем случае вместо осуществления деятельности по четкому планированию проводятся отдельные мероприятия по отработке якобы наиболее перспективных версий.

Например, при расследовании нераскрытого убийства двух женщин в частном доме в соответствующих компаниях были затребованы сведения о билинговых соединениях с помощью средств мобильной связи, находившихся во время причинения смерти вблизи от места совершения посягательства. В непосредственной близости от места преступления были расположены несколько торговых учреждений, крупная медицинская клиника, другие организации, посещаемые большим количеством людей. В результате были получены сведения о более чем 1000 соединений. Попытки выборочной проверки на причастность к преступлению некоторых пользователей аппаратов, находившихся вблизи от названного участка в момент совершения преступления, положительных результатов не принесли.

Сходные ситуации возникают и при обнаружении на месте преступления биологических следов, оставленных предположительно неустановленным субъектом преступления. Имеющиеся в настоящее время методики молекулярно-генетических исследований позволяют идентифицировать субъектов, оставивших названные следы. Вопрос состоит лишь в поиске проверяемых объектов. К сожалению, далеко не всегда сведения о разыскиваемых лицах можно получить в базах данных ДНК-учетов.

В таких ситуациях рекомендуется все-таки использовать не один, а несколько поисковых признаков личности субъекта преступления. К ним традиционно относятся свойства личности субъекта, отразившиеся в способе совершения посягательства, а через него в следах преступления. Получение такой информации позволяет отсеивать излишние данные, добытые при сплошном поиске по одному признаку, проводить иные мероприятия по проверке субъектов из охваченной версией круга лиц.

Так, при обнаружении трупа дошкольника в лесном массиве, следователи обратили внимание на некоторые негативные обстоятельства. Труп был полностью раздет, трусики и разорванная маечка пострадавшего были найдены неподалеку от трупа. В то же время на трупе не было выявлено следов сексуальных действий. Кроме того, на маечке были обнаружены следы вещества пота. В качестве одной из основных была выдвинута версия о том, что субъект преступления из числа местных жителей, страдающий психическим расстройством, в припадке внезапной ярости совершил убийство случайно встреченного им ребенка. До или после совершения убийства злоумышленник вел переговоры по имеющемуся у него аппарату мобильной связи. Для проверки этой версии были установлены пользователи аппаратов мобильной связи, которые по данным компании-оператора находились в интересующее следствие время неподалеку от места совершения убийства. Все эти лица допрашивались, освидетельствовались, у них отбирались образцы крови для идентификации по биологическим следам, оставленным на маечке. Одновременно такие же мероприятия проводились в отношении лиц, состоящих на учете в психоневрологическом диспансере. Следственные действия надлежащим образом обеспечивались оперативно-розыскным сопровождением. В итоге молекулярно-генетическая экспертиза установила, что следы на маечке оставлены местным жителем, являющимся владельцем одного из установленных аппаратов мобильной связи. В ходе проверки версии о причастности названного субъекта он был изобличен и сознался в содеянном.

Приведенный случай является примером проведения массовых поисковых мероприятий с использованием разных достижений науки и техники. При производстве таких поисков важно осуществлять жесткий контроль за своевременным и качественным выполнением запланированных оперативно-розыскных и следственных действий. Среди участников следственно-оперативной группы целесообразно назначать ответственных за выполнение контрольных функций.

При необходимости проверки десятков и сотен людей осуществлять планирование и контроль за раскрытием путем внесения отметок в планы на бумажных носителях весьма затруднительно. В этих ситуациях рекомендуется использовать средства электронно-вычислительной техники. Она позволяет кроме общего плана расследования составлять и контролировать выполнение планов проверки причастности к нераскрытому преступлению всех индивидов, относящихся к кругу лиц, к которому может принадлежать разыскиваемый субъект преступления. Сопоставление данных из нескольких планов, их взаимный контроль дают возможность своевременно выявлять случаи необоснованного отказа от проверки отдельных субъектов либо неполноты осуществляемых проверочных мероприятий. Отсутствие специальных программ, конечно, требует несколько больших затрат времени на планирование и контроль. Тем не менее имеющиеся в каждом персональном компьютере функции все-таки позволяют осуществлять рассматриваемые операции. Что же касается временных затрат, уместно напомнить, что 20 % таких затрат могут обеспечить 80 % успеха.

УДК 343.9

В.К. Кирвель

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: СОВРЕМЕННОЕ СОСТОЯНИЕ, ПРОБЛЕМЫ И ВОЗМОЖНЫЕ ПУТИ ИХ РЕШЕНИЯ

В Республике Беларусь за последние пять лет выявлено преступлений против информационной безопасности: в 2009 г. – 2154, 2010 г. – 2514, 2011 г. – 2171, 2012 г. – 2040, 2013 г. – 2558 преступлений. Можно констатировать, что количество преступлений против информационной безопасности, выявленных в Республике Беларусь, является стабильно высоким, а количество преступлений, выявленных в 2013 г., в сравнении с 2012 г. увеличилось на 25,4 %.

Увеличение количества данного вида преступлений произошло в основном за счет ст. 212 «Хищение путем использования компьютерной техники» УК Республики Беларусь. Доля преступлений данной категории от общего числа выявленных составляет более 89 %, само же количество подобных хищений увеличилось на 18,3 % (в 2011 г. – 2076, 2012 г. – 1928, 2013 г. – 2280 преступлений).

Выделяют следующие основные формы совершения преступлений по ст. 212 УК Республики Беларусь: 1) с использованием подлинных банковских платежных карточек (БПК), в РОВД и РОСК в основном встречается данный вид хищений; 2) с использованием поддельных БПК («белый пластик»); 3) с использованием реквизитов БПК, других платежных средств (идентификаторов электронных платежных систем) для совершения безналичных платежей через интерактивные платежные сервисы.

Из вышеизложенного можно выделить следующие проблемы.

1. Противоправные действия с подлинными БПК. Причины, по которым БПК выбыла из владения законного держателя и была использована для совершения хищения: 1) хищение злоумышленником БПК в составе иного похищенного имущества либо непосредственного самой БПК – около 40 % от всех преступлений; 2) утрата законным держателем БПК с написанным на ней либо на прикрепленном листке бумаги ПИН-кодом – около 20 %; 3) оставление законным держателем БПК в банкомате с введенным ПИН-кодом – около 20 %; 4) добросовестная передача законным держателем БПК другому лицу (родственнику, знакомому, коллеге и т. д.) и последующее злоупотребление злоумышленником доверием законного держателя – около 10 %; 5) иные причины – около 10 %.

Для решения указанной проблемы применяются следующие следственные и процессуальные действия: 1) осмотр места происшествия: места хищения БПК; банкомата, с использованием которого с карт-счета БПК были похищены деньги; 2) допрос потерпевшего; 3) допросы свидетелей; 4) запрос у банка-эмитента (банк, который выдал БПК) о движении (расходно-приходных операциях) по карт-счету БПК; 5) запрос у банка-эквайера (банк, который обслуживал операцию по снятию денежных средств с БПК, т. е. владелец банкомата) об операциях, осуществленных с использованием банкомата в период совершения хищения; об оборудовании банкомата средствами видеозаписи, о наличии видеозаписи в период совершения преступления; при наличии видеозаписи – производство ее выемки, последующий осмотр с целью установления личности злоумышленника; 6) запрос у компаний мобильной связи о телефонных звонках, совершенных в соте места хищения БПК в период ее хищения и в соте нахождения банкомата в период снятия с его помощью денежных средств с БПК; 7) последующий сравнительный осмотр полученных сведений для установления возможного номера мобильного телефона, которым пользовался злоумышленник; 8) при установлении личности злоумышленника – производство обыска по месту его жительства для обнаружения похищенной БПК, снятых с карт-счета БПК денежных средств или имущества, приобретенного за такие средства; 9) при наличии дактилоскопических следов – производство дактилоскопической экспертизы БПК; 10) иные следственные и процессуальные действия.

Следует иметь в виду, что похищенная БПК может быть использована не только в банкомате для снятия денег, а также в торговой точке, оборудованной специальным терминалом, для оплаты услуг или приобретения товара (без введения ПИН-кода), но и записанные на БПК реквизиты могут быть использованы для оплаты услуг и приобретения товаров в сети Интернет через специальные интерактивные платежные терминалы, например WebPay.

2. Проблема правоприменительной практики возбуждения уголовных дел. Анализ материалов с постановлениями об отказе в возбуждении уголовных дел показал, что у должностных лиц ОВД отсутствует единый подход в правоприменительной практике по делам о преступлениях, предусмотренных ст. 212 УК Республики Беларусь, совершенных с использованием БПК. Необходимо также отметить неполноту проведенных проверок по материалам из-за низкого уровня теоретических знаний и практического опыта рассмотрения таких материалов у сотрудников ОВД и отсутствие необходимых специалистов в Следственном комитете, в том числе на уровне начальников РОСК, которые оформляют отказные материалы.

Решением указанной проблемы представляется создание отделов по расследованию преступлений против информационной безопасности и интеллектуальной собственности при управление Следственного комитета или направление уголовных дел в управление по расследованию преступлений против информационной безопасности и интеллектуальной собственности при главном следственном управлении Следственного комитета.

Необходимо также отметить, что хищения денежных средств из банкоматов при помощи БПК лицами, не являющимися их держателями, сопряжены с несанкционированным доступом к компьютерной информации о карт-счетах держателей БПК и совершаются путем введения в компьютерную систему процессингового центра банка либо Банковского процессингового центра заведомо ложной информации об использовании БПК их держателями, что подлежит квалификации по ч. 2 ст. 212 УК, а при наличии соответствующих квалифицирующих признаков – по ч. 3 или 4 указанной статьи.

3. Проблема многозначности понятийного аппарата. Между юристами и техническими специалистами существует пропасть недопонимания. Специалистов, обладающих профессиональными знаниями в области информационных технологий и области права, т. е. способных перевести с технического языка на юридический язык и обратно, – единицы.

На данный момент отсутствует определенность в терминологии. Так, термины «киберпреступность», «компьютерные преступления», «преступления против информационной безопасности» и «преступления в сфере высоких технологий» – это синонимы или у них отдельное смысловое содержание? В МВД существует управление по раскрытию преступлений в сфере высоких технологий. В Следственном комитете – управление по расследованию преступлений против информационной безопасности и интеллектуальной собственности.

Термин «информация» на юридическом языке означает сведения о фактах, событиях, явлениях, предметах, процессах, представления, которые в определенном контексте имеют конкретный смысл; на научно-техническом языке – средство уменьшения неопределенности или содержание, полученное от внешнего мира в процессе приспособления к нему; на сленге – смысл, который человек приписывает данным на основании используемых им правил; на бытовом языке – сведения о чем-то, передаваемые людьми устным, письменным или другим способом.

В УК Республики Беларусь термин «информация» не определен. Законодатель отмечает, что правоприменителя должна интересовать не просто информация, а один из ее видов – компьютерная информация, однако она также не определена.

Решением указанной проблемы представляется дальнейшее совершенствование и систематизация законодательства.

УДК 393

А.А. Климов, Е.И. Климова

КРИМИНАЛИЧЕСКИЕ АСПЕКТЫ ПРОВЕРКИ И ОЦЕНКИ ДОКАЗАТЕЛЬСТВ

Высшей целью Конституция Республики Беларусь признает обеспечение прав и свобод граждан, которым государство гарантирует защиту от любых противоправных посягательств. Правовую процедуру защиты от преступных посягательств закрепляет уголовно-процессуальный закон, ее порядок определен УПК. Задачи уголовного процесса в досудебном производстве решаются путем быстрого и полного расследования преступлений, изобличения и привлечения к уголовной ответственности виновных