особенностях обстановки места преступления, в котором он может быть применен; используемых приемах, орудиях и средствах совершения преступления; образуемых ими материальных следах и местах их обнаружения.

Таким образом, в учете по способу совершения и сокрытия преступления должны быть зафиксированы поведение конкретного преступника, действия для реализации преступного замысла, которые он предпримет, сообразуясь со своим опытом, знаниями и умениями. Именно этот многообразный комплекс поступков, приемов, движений преступника в совокупности имеет криминалистическое значение, так как отражает индивидуальные особенности действовавшего лица.

В данном контексте целесообразно отметить необходимость совершенствования учетно-регистрационной деятельности в Республике Беларусь в направлении развития учета преступлений по способу их совершения.

По мнению П.П. Ищенко, существующая система учета преступлений направлена, скорее, на накопление и систематизацию криминологической и процессуальной информации. Modus operandi sistem же позволяет решить следующие задачи: установить факт совершения ряда нераскрытых преступлений одним и тем же лицом или группой лиц; выявить ряд преступлений, совершенных одним и тем же установленным лицом, привлеченным к уголовной ответственности; установить круг подозреваемых лиц по нераскрытым преступлениям.

Для большинства преступлений подойдет традиционная картотека. Компьютерная регистрация modus operandi позволяет определить степень сходства данных о подозреваемых, установить связь между преступлениями и помогает выявить наиболее вероятного преступника.

Каждая из компьютерных программ предназначена для решения определенных задач, а для modus operandi необходимо специальное программное обеспечение. Одной из основных проблем является точность компьютерных программ. Для целей modus operandi необходима гибкая программа, предусматривающая множество вариантов и возможностей.

Совершенствование учетов на основе modus operandi sistem исследователи видят в отказе от жесткой формализации помещаемой в систему информации, приведении ее в соответствие современным вычислительным технологиям. Как отмечает П.П. Ищенко, технически степень формализации определяется доступными вычислительными ресурсами и удобством пользования системой. Однако при возросших вычислительных ресурсах степень формализации учетной информации осталась прежней – на уровне 70-х гг. XX в. Учитывая, что основная информация по уголовным делам представлена в текстовом виде в документарной форме, П.П. Ищенко предлагает использовать дескрипторные информационно-поисковые языки, с помощью которых смысловое содержание документа может быть с необходимой степенью точности передано списком ключевых слов, содержащихся в тексте.

Результатом такого подхода будет электронный архив уголовных дел, в котором содержатся все основные результаты расследования, представленные в виде набора кратких формализованных данных, свободного изложения расследованного деяния на естественном языке и в семантической сети, отражающей содержание и структуру связей между элементами преступного события.

Необходимость регистрации в modus operandi sistem и использования ее в следственной работе объясняется тем, что сегодня многие опасные преступники не отбывают длительных сроков лишения свободы. Они рано освобождаются, а поэтому рано возобновляют свою преступную деятельность. Бывает, что через несколько часов после освобождения преступник совершает новое преступление привычным для него способом. В связи с этим иметь картотеку modus operandi преступников необходимо.

В современном мире розыск преступников по признакам способа совершения преступлений более чем реален. Это объясняется возможностями выявления и использования большого количества разнообразных признаков способа совершения преступления и широким применением компьютерных технологий, при помощи которых осуществляются сложные алгоритмы поиска, обусловленные вероятностным характером признаков способа совершения преступления.

УДК 343.982.35

И.А. Шаматульский

ОСОБЕННОСТИ МЕХАНИЗМА ОБРАЗОВАНИЯ СЛЕДОВ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Механизм образования следов киберпреступлений характеризуется особенностями способов подготовки, совершения и сокрытия данных преступлений, в основе которых лежат технологии дистанционной передачи информации с использованием телекоммуникационных и компьютерных сетей.

Можно выделить следующие группы следов преступлений, связанных с использованием средств компьютерной техники:

следы на средствах компьютерной техники, с помощью которых было совершено преступление (использовавшееся для неправомерного доступа программное обеспечение, сохраненные коды доступа, скопированная у потерпевшей стороны информация, тексты программ и т. п.), такие следы могут остаться в записях операционной системы, на электронных носителях, в аппаратно-программной конфигурации компьютерных средств и др.;

следы на «транзитных» носителях информации, посредством которых лицо осуществляло связь с удаленными информационными системами или ресурсами (размещенная в сети информация, электронная переписка и др.);

следы в подвергшейся воздействию компьютерной системе, в том числе на электронных носителях (результаты неправомерного уничтожения, блокирования, модификации компьютерной информации, воздействия на средства защиты информации и несанкционированного доступа к компьютерной системе);

следы на иных компьютерных средствах (компьютеры, органайзеры, мобильные телефоны, цифровые фотоаппараты, видеокамеры, диктофоны, другие носители информации), непосредственно не участвовавших в совершении преступления, но содержащих имеющие значение для уголовного дела сведения;

документы, изготовленные с использованием средств компьютерной техники;

традиционные следы – материальные (следы рук, обуви, орудий, инструментов и др.) и идеальные (отображение события в сознании человека, в этом случае криминалистически значимая информация может быть воспроизведена в вербальной или иной форме, например в качестве свидетельских показаний).

На месте происшествия можно обнаружить как «традиционные», так и цифровые следы, остающиеся в памяти электронных устройств, принадлежащих потерпевшим и преступникам. При расследовании киберпреступлений наибольшей спецификой обладают цифровые следы преступления. Они представляют собой результаты создания или преобразования компьютерной информации в форме уничтожения, копирования, блокирования или модификации, а также соответствующие им изменения физических характеристик ее носителя, связанные с событием преступления.

Анализ цифровых следов при расследовании киберпреступлений имеет большое значение. С помощью специальных автоматизированных систем можно собирать информацию об интернет-активности интересующего правоохранительные органы человека (фиксируются места посещения интернет-ресурсов, переписка в сети Интернет, объекты платежей и др.). Эти следы являются идеальными невидимыми следами, но материально закрепленными на носителе. Они не имеют ни формы, ни цвета, ни запаха – в этом и состоит сложность их фиксации и изъятия органами уголовного преследования. Сам след представляет собой сложную информационную структуру, которая помимо значимых данных содержит в себе большой объем информации, позволяющей идентифицировать ее среди других сведений, размещенных на различных электронных носителях, а также интегрировать ее в целостную информационно-коммуникационную сеть и базы данных.

Существуют два вида цифровых следов:

активный цифровой след – данные, которые человек сознательно «отдает», когда соглашается принять cookie, пишет комментарии, текст, выкладывает фото-, видеоизображения, ставит лайки и делает репосты, из этого складывается виртуальный образ личности;

пассивный цифровой след – оставляется пользователем непредумышленно, это данные историй посещений, сведения об устройстве и IP-адрес, этот цифровой след контролировать невозможно.

Следами-предметами при совершении киберпреступлений являются само компьютерное оборудование с имеющимися в нем микросхемами и составными частями, пластиковые карты, средства мобильной связи и др. Указанные объекты только тогда имеют значение, когда в них находится информация, непосредственно связанная с интересующим следствие событием и имеющая доказательственное значение.

Необходимо учитывать, что любые операции с компьютерной техникой, средствами мобильной связи и т. п. находят отражение в памяти указанных устройств, а именно: включение и выключение устройства, операции с информацией в памяти компьютерного устройства отображаются в журналах администрирования; манипуляции с программами – в реестре компьютерной техники; сведения о работе в сети Интернет, а также в локальных сетях – в log-файлах; операции с файлами – в свойствах файлов.

Отличительными чертами цифровых следов являются неявный вид и необходимость использования специальных средств для обеспечения ее восприятия; возможность уничтожения или модификации в кратчайшие сроки и удаленно; наличие специальных средств, ограничивающих доступ к данной информации; постоянное изменение информации в ходе работы пользователя и выполнения различных операций; формирование взаимосвязанной информации на различных устройствах одновременно при передаче данных по каналам связи.

Указанные свойства цифровых данных обусловливают необходимость соблюдения определенных правил при фиксации и изъятии цифровых доказательств, а также при их судебно-экспертном исследовании.

УДК 343.1

Я.А. Шараева

ПРОБЛЕМЫ, ВОЗНИКАЮЩИЕ НА ЭТАПЕ ОКОНЧАНИЯ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ В ФОРМЕ ДОЗНАНИЯ

Этап окончания уголовного дела и формирования обвинительного акта дознавателем является достаточно трудоемким с учетом обладания им процессуальными полномочиями, закрепленными УПК РФ. На данном этапе дознаватель встречается с множеством препятствий и проблем, например с противодействием стороны защиты, выражающимся в затягивании срока расследования по уголовному делу. С таким препятствием дознаватель встречается при уведомлении стороны защиты об окончании предварительного расследования. В целях экономии рабочего времени и сокращения срока расследования дознавателю очень помогло бы использование оповещения в формате SMS, но сегодня такой формат не урегулирован УПК РФ, а используется только на судебных стадиях рассмотрения уголовного дела.

В полномочия дознавателя входит применение привода в отношении обвиняемого, если тот целенаправленно и без уважительной причины не является к нему по вызову. Однако если защитник не будет являться к дознавателю, то в данном случае у дознавателя нет средств воздействия на него в целях пресечения умышленного затягивания срока расследования.