Особенности тактической операции при расследовании НУПВ заключаются в ее подготовке и проведении (осуществляется следователем по единому плану), проведении для решения какой-либо одной сложной задачи расследования, ее содержании (могут входить в полном объеме либо фрагментами отдельные следственные действия, организационные, ревизионные, оперативно-розыскные мероприятия), полученных в результате ее проведения имеющих доказательственное значение по делу сведениях.

При расследовании НУПВ возникают следующие сложные задачи:

определение объекта и объективных признаков НУПВ; отношений подчиненности лиц, участвующих в данных правонарушениях; сведений об этапах прохождения срочной военной службы;

установление способов подготовки, совершения и сокрытия данных преступлений; преступных действий, образующих НУПВ, характера их проявлений; следов НУПВ; времени и места совершения преступления;

установление личности потерпевшего, свидетелей и иных категорий военнослужащих по делу;

установление последствий НУПВ, квалифицирующих обстоятельств (признаков), наличия телесных повреждений у потерпевших и др.;

профилактическая деятельность и др.

Таким образом, тактические операции представляют собой одно из перспективных тактико-криминалистических средств повышения эффективности расследования НУПВ, в содержание которых входят организационные, технические, оперативно-розыскные и иные мероприятия.

УДК 343.985

С.С. Сенькевич

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В КРИМИНАЛИСТИКЕ

Развитие информационных технологий обусловило не только появление новых видов преступлений в виртуальной среде, получивших название киберпреступлений, но и трансформацию способов совершения «традиционных» преступлений. В свете современных тенденций криминалистика активно осваивает и разрабатывает новые подходы к их изучению, осуществляемые с использованием передовых информационных технологий. Это новое направление активно формируется и развивается. В научной среде не прекращаются споры по определению его места в системе криминалистики или о выделении в самостоятельное научное направление – форензику.

Анонимность, которую предоставляет сеть Интернет, обусловливает определенные трудности, связанные с расследованием киберпреступлений. Одной из таких проблем является недостаточность виртуальных следов, которые могли бы помочь в идентификации личности преступника. Киберпреступники, как правило, действуют на значительном расстоянии от своих жертв, часто – на территории другого государства. Это создает дополнительные трудности по установлению лиц, совершающих такие преступления, а также для проведения качественного расследования.

В отличие от традиционных следов виртуальные следы легко изменяются и уничтожаются. Это обстоятельство обусловливает важность быстрого обнаружения и оперативного исследования таких следов. С данной целью применяются специализированные знания в области информационных технологий и технико-криминалистических средств для эффективного раскрытия и расследования киберпреступлений. В этом контексте важно отметить, что развитие новых методов и технологий, таких как искусственный интеллект и машинное обучение, может значительно облегчить процесс обнаружения и анализа виртуальных следов.

С одной стороны, цифровая информация хранится на материальных носителях, обладающих конкретными физическими свойствами, таких как жесткие диски и флеш-карты. Однако, с другой – цифровая информация является продуктом интеллектуальной работы человека, и ее можно обнаружить только с помощью специализированных технических устройств, а исследование требует специфических знаний.

Программные комплексы, используемые в криминалистике для анализа цифровых следов, включают в себя средства для извлечения и анализа данных с электронных устройств (EnCase, FTK (Forensic Toolkit), XRY, Oxygen Forensic Detective и т. д.), инструменты для анализа интернет-активности (Internet Evidence Finder, Web Historian и т. д.), программное обеспечение для восстановления удаленных файлов и артефактов (например, Disk Drill, Recuva).

В технические комплексы входят оборудование и инструменты, используемые для сбора и анализа цифровых следов, например клонирование носителей информации с помощью программно-аппаратных средств, таких как комплекты для снятия образов дисков (кардридеры, write blockers); средства для анализа мобильных устройств, включая программаторы (Cellebrite, UFED).

Кроме того, существует целый ряд технических средств, таких как устройства для считывания информации с SIM-карт, искатели скрытых камер и аудиоустройств, а также специальное оборудование для анализа сложных цифровых устройств, например авионики, медицинского оборудования и автомобильных компьютеров.

В этом аспекте следует констатировать ряд промежуточных выводов:

криминалистика является одной из основных дисциплин, которая занимается изучением методов и средств борьбы с киберпреступностью;

для эффективной борьбы с преступностью необходимо использовать комплексный подход, включающий в себя не только оперативную работу правоохранительных органов, но и научные исследования в области криминалистики;

одной из главных задач криминалистики является разработка новых методов и технических средств, которые позволят более эффективно раскрывать киберпреступления;

важным направлением развития криминалистики является разработка системы профилактики киберпреступлений, которая позволит предотвратить совершение таких преступлений и снизить уровень преступности в обществе;

криминалистика играет важную роль в судебной практике, поскольку ее методы и средства используются при судебном разбирательстве;

в настоящее время необходимо уделить особое внимание развитию информационных технологий в криминалистике, которые позволят собирать и анализировать большие объемы данных, что, в свою очередь, будет способствовать более эффективному раскрытию преступлений.

К основным направлениям использования информационных технологий в криминалистике относятся:

цифровая криминалистика – использование информационных технологий для сбора, сохранения и анализа цифровых следов, которые могут быть использованы в качестве доказательств в суде;

сетевое направление – исследование преступлений, совершенных в сети Интернет, включая киберпреступления (мошенничество, хакерские атаки и распространение вредоносного программного обеспечения);

биометрическое направление – использование биометрических технологий, позволяющих получить сведения о преступниках (отпечатки пальцев, распознавание лиц и голоса и т. д.);

геоинформационное направление – применение ГИС-технологий для производства следственных действий и проведения оперативно-розыскных мероприятий;

анализ преступлений и прогнозирование преступности (цифровая криминалистическая модель преступлений определенного вида, определение криминалистического поискового портрета и т. д.);

криминалистический анализ данных – применение методов анализа данных и машинного обучения для выявления закономерностей и обнаружения криминальной активности в сети Интернет.

Эти направления являются ключевыми в современной криминалистике и продолжают развиваться с учетом быстрого темпа эволюции информационных технологий.

Таким образом, информационные технологии могут повысить эффективность и качество применения криминалистической техники, обеспечивая быстрый и эффективный поиск следов преступлений, их предварительное изучение, автоматизацию рутинных процессов, интеграцию различных источников информации, создание баз данных и экспертных систем, применение искусственного интеллекта и машинного обучения.

Для успешного внедрения информационных технологий в криминалистическую науку необходимо решить ряд проблем, таких как недостаток финансирования, отсутствие единых стандартов и нормативов, нехватка квалифицированных специалистов, низкий уровень информационной безопасности, юридические и этические ограничения, сопротивление изменениям со стороны сотрудников правоохранительных органов.

Перспективы внедрения информационных технологий в криминалистику связаны с развитием биометрии, цифровой криминалистики, цифрового профайлинга, виртуальной и дополненной реальности, нейрокриминалистики, генетической инженерии, нанотехнологий и др. Эти технологии могут открыть новые возможности для идентификации, реконструкции, моделирования и прогнозирования преступного поведения.

УДК 343.98

А.Е. Середа

КРИМИНАЛИСТИЧЕСКАЯ ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ ЧЕЛОВЕКА ПО БИОМЕТРИЧЕСКИМ ПРИЗНАКАМ ЛИЦА

Идентификация личности человека по биометрической характеристике лица является одним из динамично развивающихся направлений научной мысли. Данная область условно делится на две основных сферы применения технологий: 2D- и 3D-распознавание. Удельный вес технологий распознавания по геометрии и признакам лица в общем объеме мирового биометрического рынка находится в пределах 13–18 %. Лидерами в настоящий момент являются системы Visionic, Viisage и Miros.

Развитием данной технологии занимаются Geometrix, Inc. (3D-сканеры лица, программное обеспечение), Genex Technologies (3D-сканеры лица, программное обеспечение) в США; Cognitec Systems, GmbH (SDK, вычислители, 2D-камеры), Bioscrypt (3D-сканеры лица, программное обеспечение) в Германии; Artec Group (3D-сканеры, программное обеспечение) в России; Synesis в Беларуси. Международный подкомитет по стандартизации в области биометрии (IS0/IEC JTC1/SC37 Biometrics) по состоянию на 2024 г. осуществляет разработку единого формата сведений для распознавания человеческих лиц на основе двух- и трехмерных изображений.

С целью создания модели лица система находит опорные антропометрические точки, определяющие его индивидуальные характеристики. На лице выделяются контуры бровей, глаз, носа, губ и т. д., вычисляется расстояние между ними и строится не просто образ, а множество его вариантов в случае поворота лица, наклона головы и изменения выражения психоэмоционального состояния на лице. Количество моделируемых образов варьируется в зависимости от целей использования.

Минимальное количество опорных точек составляет 68 единиц, однако в некоторых системах их количество составляет 200 единиц и более. В общем случае подобная биометрическая система хранит не фотографии, а наборы цифр, характеризующих лицо, т. е. модель-дескриптор. Идентификация осуществляется путем сравнения полученной системой в процессе работы биометрической модели с хранящимся в базе дескриптором.