Степень сходства лица показывает процент, при котором программная платформа будет создавать событие о найденном человеке (на сколько, по мнению программы, зафиксированное камерой лицо похоже на разыскиваемого).

Достаточно эффективно использование РСМОБ в части распознавания лиц показало себя при установлении личности курьеров так называемых телефонных мошенничеств, когда последние получали, как правило, от лиц пожилого возраста деньги для их последующей передачи (перевода) организаторам преступной деятельности.

2. Распознавание дорожной обстановки с целью детектирования транспортных средств, их цвета, типа, регистрационных знаков разыскиваемых автомобилей. Обеспечивает решение задач контроля, регистрации и идентификации автомобилей на любых объектах, для которых характерен транспортный поток различной интенсивности. Используется для контроля транспортных средств, розыска угнанных автомобилей. Программный модуль системы распознает государственные регистрационные знаки автомобилей из более чем 20 стран мира.

Возможности РСМОБ также позволяют выявлять транспортные средства, владельцы которых лишены права управления, осуществлять контроль за соблюдением установленных ограничений со стороны лиц, состоящих на различных учетах (в уголовно-исполнительных инспекциях, в подразделениях гражданства и миграции и др.).

3. Слежение за объектами. Используется:

1) для обнаружения людей, транспортных средств, оставленных предметов в зоне наблюдения;

2) для охраны периметра объектов особого назначения (границы, склады, исправительные учреждения и др.), промышленных и производственных предприятий, автозаправок, объектов здравоохранения, школ, детских садов.

Детектирование оставленных предметов (бесхозных или забытых вещей) позволяет бороться с появлением в зоне наблюдения предметов, потенциально угрожающих безопасности, например, взрывных устройств. С помощью системы устанавливаются владельцы оставленного имущества. Кроме этого, модули РСМОБ реагируют на возникающее задымление, различные звуки (крики, шумы, выстрелы и т. п.).

Направления развития РСМОБ в целях борьбы с преступностью:

1) увеличение количества устанавливаемых видеокамер, в том числе обзорных, улучшение их технических характеристик;

2) развитие подъездного видеонаблюдения;

3) совершенствование программного обеспечения системы, расширение возможностей модулей для видеоаналитики.

Таким образом, несмотря на то, что появление РСМОБ в основном связано с необходимостью повышения уровня общественной безопасности путем использования современных информационно-коммуникационных технологий, сегодня ее возможности активно используются в раскрытии и расследовании преступлений, в первую очередь уличных (краж, мошенничеств, умышленных причинений тяжких телесных повреждений, хулиганств и др.).

УДК 343.575

С.В. Тимофеев

ОРГАНИЗАЦИОННО-ТАКТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Повсеместное использование достижений технического прогресса во всех сферах жизни человечества привело к тому, что информационные технологии не только способствовали повышению экономического потенциала стран мира, но и поспособствовали тому, что преступники совершенствовали способы сокрытия преступлений, обеспечению мер конспирации и анонимизации личности. Это привело к тому, что в последнее двадцатилетие в российском государстве произошел буквально взрывной рост числа преступлений, совершаемых в сфере информационно-коммуникационных технологий (ИКТ).

Официальная статистика ГИАЦ МВД России наглядно показала негативную динамику ежегодного роста числа преступлений, совершаемых с использованием ИКТ. Так, за январь – декабрь 2022 г. в Российской Федерации из 1 966 795 зарегистрированных преступлений 522 065 относятся к данной категории, т. е. каждое четвертое совершено с использованием ИКТ. Обозначенная динамика увеличения количества преступлений данной категории прослеживается и в 2023 г. За январь – август зафиксирован рост противоправных деяний в сфере ИКТ на 28,7 %. Их удельный вес в числе всех преступных посягательств возрос до 32,9 %, а по тяжким и особо тяжким – до 56,4 %. Больше совершено дистанционных мошенничеств и краж. Раскрываемость киберпреступлений составила 29,9 %, в том числе совершенных с использованием сети Интернет – 28,8 %, расчетных (платежных) карточек – 35,7 %.

Как справедливо отметил А.В. Варданян, «анализ оперативно-розыскной, следственной и судебной практики показал наличие серьезных проблем в научной обеспеченности цифровых методов предупреждения, раскрытия, расследования дистанционных хищений. В первую очередь это связано с нехваткой разработок в теории оперативно-розыскной деятельности и, соответственно, науке криминалистики».

Общество и государство должным образом отреагировали на современные вызовы подрыва основ безопасности, связанные с киберпреступностью. В этой связи Указом Президента Российской Федерации В.В. Путина от 30 сентября 2022 г. № 688 «О внесении изменений в некоторые акты» в структуре Министерства внутренних дел Российской Федерации было создано новое оперативное подразделение – Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК). Приказом Министра внутренних дел Российской Федерации В.А. Колокольцева от 31 марта 2023 г. № 199 «Об утверждении перечня оперативных подразделений органов внутренних дел Российской Федерации, правомочных осуществлять оперативно-розыскную деятельность» подразделения УБК стало полноправным субъектом оперативно-розыскной деятельности.

С учетом обозначенных факторов, в целях совершенствования мер по борьбе с киберпреступлениями, остро назрел вопрос о подготовке квалифицированных сотрудников для оперативных подразделений органов внутренних дел по борьбе с противоправным использованием ИКТ. В современных условиях это предполагает проведение тщательного анализа современных проблем борьбы с киберпреступностью, разрешение которых невозможно без осмысления тенденций развития теоретической юридической науки, законодательства и практики его применения. В этой связи логично обратиться к некоторым из них.

Во-первых, до недавнего времени в правовом регулировании общественных отношений Российской Федерации в сфере кибербезопасности наблюдались противоречивые процессы. С одной стороны, из законодательства постепенно вымываются нравственные начала в силу его нормативности, требований юридической техники и формальной определенности. В результате принципы справедливости и гуманности в некоторых случаях носят декларативный характер, все чаще правоохранители вынужденно прибегают к ограничению прав граждан (например, право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений), увеличивается разрыв между правом и человеком. Это влияет на состояние законности и правопорядка, способствует распространению нигилистических идей в обществе. С другой – в условиях господства законодательных ограничений все более очевидным проявляется в современном законодательстве.

Во-вторых, наличие проблемы отставания уровня знаний в области функционирования сетей передачи цифровых данных, в том числе в теневом сегменте сети Интернет – DarkNet, и необходимость практической подготовки сотрудников оперативных подразделений к противодействию явлению киберпреступности. Эта проблема появилась и существует с момента возникновения первых цифровых технологий, приобрела гипертрофированный характер. Часто, имея юридическое образование, сотрудники полиции ограничены в возможности своевременного и эффективного принятия соответствующих мер защиты граждан от преступлений, совершаемых с использованием ИКТ.

В-третьих, как справедливо отмечает А.В. Григорьев, общественные отношения настолько динамичны, что законодатель не в силах спрогнозировать возможные проблемы в будущем, а также своевременно отреагировать на имеющиеся, что особенно актуально для правоохранительных органов в части борьбы с цифровой преступностью. В этой связи возникает острая необходимость в совершенствовании законодательства и правоохранительной деятельности, подготовке высокопрофессиональных кадров для правоохранительных органов.

В-четвертых, наличие в оперативно-розыскном законодательстве норм, ограничивающих проведение оперативно-розыскных мероприятий разведывательного характера в сети Интернет без отсутствия формальных оснований, предусмотренных ст. 7 Федерального закона Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности». Обозначенная ситуация подтверждает позицию о некотором отставании законодателя в части урегулирования общественных отношений от их динамичного развития. Вместе с тем в российском правоведении на смену существовавших многие десятилетия методологии и догматизму приходит многообразие научных направлений. Появляются первые научные исследования в области цифровых следов преступлений и их использования в уголовном судопроизводстве, которые и направлены на устранение возникающих пробелов в законодательстве. В результате стало очевидным, что понятийно категориальный аппарат теоретической юридической науки требует дальнейшего развития. При этом многие современные проблемы правовой реальности носят не только объективный, но и субъективный характер.

Создание нового субъекта оперативно-розыскной деятельности органов внутренних дел – УБК – дает основание полагать, что взрывной рост киберпреступности, отмеченный в последние годы в Российской Федерации, будет эффективно и своевременно купирован. Решению этой задачи будут способствовать подготовка высококвалифицированных сотрудников для этого подразделения, разработка научно обоснованных методик и программ, способных решить проблему эффективного оперативно-розыскного противодействия киберпреступности.

УДК 343.985.8

А.Н. Толочко

МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ К ПРОВЕДЕНИЮ КОЛИЧЕСТВЕННОГО АНАЛИЗА МЕЖДИСЦИПЛИНАРНЫХ И МЕЖПРАКТИЧЕСКИХ СВЯЗЕЙ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ МАТЕМАТИЧЕСКИХ МЕТОДОВ ОБРАБОТКИ ДАННЫХ

Одним из возможных методологических подходов к исследованию междисциплинарных (МД) связей в научной сфере и межпрактических (МП) связей в практической сфере является подход, основанный на использовании особого математического инструментария – матриц, представляющих собой специальным образом построенные (заполненные) таблицы, позволяющие определять количественные (числовые) характеристики МД и МП связей. Ранее матричный метод применялся в сфере образования при исследовании связей между учебными дисциплинами.

При исследовании связей между учебными дисциплинами используются матрицы логических связей. Рассмотрим для примера порядок построения матрицы логических связей между разделами двух разных учебных дисциплин – А и В. Дисциплина В является опирающейся, она для своего усвоения нуждается в предварительном изучении дисциплины А, которая является опорной. Каждому разделу присваивается номер, установленный в порядке последовательности изучения разделов дисциплин. Составляется матрица – прямоугольная таблица, строками которой являются пронумерованные разделы дисциплины В, а столбцами – пронумерованные разделы дисциплины А. На пересечениях строк и столбцов ставится знак «+» или цифра «1», если имеется наличие связей между разделами. Если связей между разделами нет, то на пересечениях строк и столбцов ставится цифра «0» или оставляется пустое место.