ка междисциплинарного мышления и принятия соответствующего уровня решений требуется реализация междисциплинарных технологий.

Примером внедрения в образовательный процесс междисциплинарных технологий в Нижегородской академии МВД России служат практические занятия по предупреждению коррупции в органах внутренних дел и формированию антикоррупционного поведения сотрудников и работников органов внутренних дел.

Реализация научно-педагогической концепции кафедры криминалистики Нижегородской академии МВД России предполагает соблюдение строгой последовательности изучения обучающимися курса криминалистики с учетом приведенной выше методики формирования криминалистического стиля мышления; определение в курсе криминалистики места алгоритма криминалистического анализа информации; разработку современных (инновационных) педагогических технологий, дидактических материалов, средств доставки учебного материала, позволяющих совершенствовать процесс формирования криминалистического стиля мышления; развитие форм педагогического контроля знаний, оценочных средств; формирование соответствующего современным реалиям методического обеспечения образовательного процесса.

1. Криминалистика : курс лекций / под ред. А.Ф. Лубина. Н. Новгород, 2018.

2. Журавлев С.Ю. О дидактических подходах к формированию аналитического мышления в ходе проведения практических занятий по криминалистике // Криминалистика: проблемы методологии и практики расследования отдельных видов преступлений : сб. науч. ст. / под ред. А.Ф. Лубина. Н. Новгород, 2003.

3. Журавлев С.Ю. Основы формирования криминалистического стиля мышления субъекта расследования преступлений // Современная криминалистика: проблемы, тенденции, имена (к 90-летию профессора Р.С. Белкина) : сб. материалов 53-х криминалист. чтений : в 3 ч. М., 2012. Ч. 1.

4. Гуслова М.Н. Инновационные педагогические технологии : учеб. пособие. 3-е изд., испр. М., 2012.

УДК 347.973

М.Г. Жук

ФОРМИРОВАНИЕ КРИМИНАЛИСТИЧЕСКОЙ МЕТОДИКИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Современное общество невозможно представить без компьютерных технологий, уровень которых постоянно растет. Они проникли практически во все сферы жизни. Одновременно возрастает и количество,

противоправных посягательств в этой сфере, появляются новые средства и способы совершения преступлений. По данным МВД Республики Беларусь, в 2017 г. выявлено 3 099 преступлений в сфере высоких технологий, что на 25,4 % больше в сравнении с 2016 г. При этом рост числа таких уголовно наказуемых деяний отмечается во всех регионах страны. Особенностью компьютерных преступлений является их транснациональный характер. Уже не имеют большого значения границы между странами, расстояния, разница в языках общения. Определяющими становятся уровень компьютеризации общества, возможность доступа к компьютерам, соответствующие специальные знания, общие для программистов разных стран.

Понятие «преступление с сфере высоких технологий» для уголовного права и криминалистики сравнительно новое. Термин сложился стихийно для удобства обозначения преступлений, орудием или предметом которых стала компьютерная информация или компьютерные средства. В 80-х гг. XX в. данные преступления достигли такого распространения, что в национальных правовых системах, а затем и на международном уровне были приняты правовые нормы, вводившие уголовную ответственность за их совершение [1, с. 6].

Орудием совершения компьютерного преступления могут являться как компьютерные средства и оборудование, так и программное обеспечение, с помощью которого преступники осуществляют неправомерный доступ к охраняемой компьютерной информации. Не всякий неправомерный доступ образует состав преступления, а лишь такой, при котором наступили вредные последствия для правообладателя информации, затруднившие или сделавшие невозможным для потерпевшего использование информации: уничтожение, блокирование, модификация или копирование информации [2, с. 617]. Такие деяния получили названия «компьютерные преступления», «киберпреступления», «преступления в сфере высоких технологий», «высокотехнологичные преступления», «преступления в сфере компьютерной информации», «сетевые преступления», «машинно-интеллектуальные преступления», «технико-интеллектуальные преступления», в основном подразумевающие одни и те же виды преступной деятельности [3, с. 6]. Наибольшее распространение в отечественной юридической литературе получил термин «компьютерные преступления».

Компьютерное преступление – противозаконная деятельность, связанная с информационными ресурсами, при которой компьютер выступает либо как объект совершения преступления, любо как субъект непосредственного воздействия. Главная особенность компьютерных преступлений – это сложность в установлении состава преступления и

решении вопроса о возбуждении уголовного дела. Компьютерная информация способна достаточно быстро изменять свою форму, копироваться и пересылаться на любые расстояния. Следствием этого являются трудности с определением первоисточника и субъекта совершения преступления. Информация как криминалистический объект имеет ряд специфических свойств: высокая динамичность, постоянное функционирование, возможность дистанционной работы и, безусловно, возможность быстрого изменения и безвозвратного удаления большого объема данных. Получив доступ к информации, киберпреступник может использовать все известные ему средства для манипулирования поведением объекта преступления. Основными факторами, способствующими совершению компьютерных преступлений, являются: низкий уровень прикладного программного обеспечения; наличие возможности несанкционированного доступа или модификации компьютерной информации; концентрация компьютерной информации различного назначения в единых базах данных; отсутствие надлежащего контроля за доступом к информации; небрежность пользователей ЭВМ, несоблюдение мер предосторожности; постоянное увеличение потоков информации, накапливаемой, хранимой и обрабатываемой при помощи компьютеров и других средств автоматизации [4, с. 42–45].

В процессе формирования основ криминалистической методики расследования преступлений в сфере компьютерной информации возникают определенные сложности: высокая латентность, достигающая по разным оценкам порядка 90 %; сложность сбора доказательств и процесса доказывания в суде ввиду отсутствия достаточной следственной практики; широкий спектр криминалистически значимых признаков этих преступлений; несовпадение места совершения противоправных действий и места наступления общественно опасных последствий; механизм совершения скрыт от правоохранительных органов.

Затрудняет следствие и то, что компьютерные преступления общественным мнением не рассматриваются порой как серьезная угроза.

Получение и анализ доказательств по делам о преступлениях в сфере компьютерной информации – одна из основных и трудно решаемых на практике задач. Ее решение требует не только особой тактики проведения следственных и организационных мероприятий, но и наличия специальных познаний в области компьютерной техники и программного обеспечения. При расследовании компьютерных преступлений следователь сталкивается с необходимостью выявления и изъятия следов и собирания доказательств на таких объектах исследования, как компьютерная система, телекоммуникационная сеть или носитель информации (магнитный, оптический и т. д.). При этом в некоторых случаях

приходится искать нечто неосязаемое, а не привычные физические улики в виде следов применения оружия, отпечатков пальцев, поддельных документов. Основные проблемы связаны с описанием подлежащего изъятию компьютерного оборудования и компьютерной информации, а также с тактикой проведения обыска. Особые сложности при производстве следственных действий возникают в случае распределенных компьютерных систем обработки информации, так как место совершения преступления часто не совпадает с местом происшествия и наступления преступного результата [5, с. 265–270].

Разработка теоретических основ расследования преступлений в сфере компьютерной информации сложна и имеет много аспектов на стыке права, теории информатики, производства и эксплуатации аппаратных средств компьютерных систем, сетей и иного сопряженного оборудования.

Для разработки методики расследования компьютерных преступлений большое значение имеет их криминалистическая структура, которая включает следующие элементы: предмет посягательства, орудие посягательства, физическая деятельность субъекта, вредные последствия, место и время совершения преступления, субъект преступления, психическая деятельность субъекта. Основным предметом посягательства является компьютерная информация, определяемая как документированные сведения о лицах, предметах, фактах, событиях, явлениях и процессах, хранящиеся на машинных носителях, в ЭВМ, системе или сети ЭВМ либо управляющие ЭВМ [3, с. 64].

Способ совершения преступления слагается из комплекса специфических действий правонарушителя по подготовке, совершению и маскировке преступного посягательства. Нередко эти действия представляют собой целую систему со многими ее элементами и оставляют во внешней обстановке соответствующие отражения, составляющие информационную модель преступления [6, с. 69–70].

Можно быть выделить следующие основные обстоятельства, подлежащие обязательному установлению и доказыванию по делам рассматриваемой категории:

имело ли место компьютерное преступление (либо это правонарушение иного рода);

каков объект преступного посягательства (данное обстоятельство имеет решающее значение для применения следователем той или иной методики расследования конкретного преступления или их совокупности преступлений);

каков предмет преступного посягательства;

каков способ совершения преступления;

место, время (период) и обстоятельства совершения преступления;

вид и размер ущерба, причиненного пострадавшему;

кто совершил преступление;

если преступление совершено группой лиц, то каковы состав группы и роль каждого соучастника;

какие обстоятельства способствовали совершению преступления.

В настоящее время наиболее полно, на наш взгляд, разработана методика расследования неправомерного доступа к компьютерной информации. Алгоритм расследования этого преступления построен по следующей схеме:

1) установление самого факта неправомерного доступа к информации в компьютерной системе или сети;

2) установление места несанкционированного проникновения в компьютерную систему или сеть;

3) установление времени несанкционированного доступа;

4) установление надежности средств защиты компьютерной информации;

5) установление способа несанкционированного доступа;

6) установление лиц, совершивших неправомерный доступ к компьютерной информации;

7) установление виновности и мотивов лиц, совершивших неправомерный доступ к компьютерной информации;

8) установление вредных последствий неправомерного доступа к компьютерной системе или сети;

9) выявление обстоятельств, способствовавших неправомерному доступу к компьютерной информации.

Как отмечает И.А. Возгрин, программы (алгоритмы) расследования данного вида преступлений должны строиться поэтапно (наиболее подробно для первоначального этапа, начиная с момента получения первичной информации и обнаружения признаков преступления), по наиболее часто встречающимся следственным ситуациям, с учетом выдвигаемых в каждой из них типичных следственных версий. Они должны включать научно обоснованную систему следственных, оперативно-розыскных, организационно-технических и иных действий и мероприятий, направленных на быстрое и полное установление истины по уголовному делу [7, с. 29].

1. Вехов В.Б., Попова В.В., Илюшин Д.А. Тактические особенности расследования преступлений в сфере компьютерной информации. М., 2004.

2. Крылов В.В. Расследование преступлений в сфере компьютерной информации. М., 1998.

3. Кушниренко С.П. Методика расследования преступлений в сфере высоких технологий : конспект лекций. СПб., 2007.

4. Хомколов В.П. Предупреждение преступлений в сфере компьютерной информации // Право: теория и практика. М., 2004.

5. Мещеряков В.А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста. 2013. № 5.

6. Вехов В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники : дис. … канд. юрид. наук. Волгоград, 1995.

7. Возгрин И.А. Научные основы криминалистической методики расследования преступлений. СПб., 1993. Ч. 4.

УДК 343.98

Н.Н. Ильин

ПРЕДПОСЫЛКИ СОЗДАНИЯ ЧАСТНОЙ ТЕОРИИ ТРАНСПОРТНО-ТЕХНИЧЕСКИХ СУДЕБНЫХ ЭКСПЕРТИЗ

Происшествия, совершенные на воздушном, водном и железнодорожном транспорте, вызывают большой общественный резонанс, и им всегда уделяется пристальное внимание в средствах массовой информации. Так, в России за последние годы значительно возросло число авиационных происшествий. Если в 2007 г. было 7 авиапроисшествий, в 2017 г. – 38. По данным Межгосударственного авиационного комитета, с 2007 г. по 2017 г. в России произошло 202 авиационных происшествия и 173 катастрофы [1]. На дорогах количество погибших также остается на очень высоком уровне. По данным ГИБДД, за 2017 г. количество погибших в результате ДТП составило 19 тыс. человек. В этой связи Президент Российской Федерации на расширенном заседании коллегии МВД России говорил о необходимости внедрения новых технологий безопасности, применения современных средств фиксации нарушений и улучшения механизмов взаимодействия с другими ведомствами для последовательного сокращения количества транспортных происшествий и смертности на дорогах [3].

Следует отметить, что сегодня участились случаи использования заведомо технически неисправных транспортных средств, что нередко приводит к авариям, катастрофам и другим происшествиям на различных видах транспорта. Создание эффективной системы борьбы с преступлениями против безопасности движения и эксплуатации транспорта предполагает полное и всестороннее изучение причин и условий совершения преступлений, совершенствование методики их расследования с использованием в том числе специальных знаний в форме судебной экспертизы.