необходимость в усовершенствовании имеющихся оперативно-розыскных методик противодействия отдельным видам преступлений, а в случае отсутствия таковых – в разработке новых.

Для успешного развития вышеуказанных методик и повышения их эффективности осуществляется в первую очередь познание закономерностей совершения общественно опасных деяний, возникающих связей и отличительных признаков, обусловленных фактором человеческого воздействия на окружающую действительность. Основу приобретения нужных знаний составляют исследования характеристик преступлений в уголовном праве, криминологии, криминалистике, теории оперативно-розыскной деятельности. Вместе с тем каждая из перечисленных наук ограничивается предметом изучения, а значит, рассматривает преступление с позиции собственного интереса.

Практические рекомендации по выявлению и раскрытию преступлений традиционно базируются на оперативно-розыскной характеристике, позволяющей установить процесс формирования следов в результате выявления особенностей поведения преступника. Это помогает оперативному сотруднику ограничить поисковые направления, выстроить логическую последовательность выбора своих действий и рационально их реализовать для достижения поставленной цели. Особую актуальность обозначенная характеристика приобретает в ходе изобличения лиц, которые причастны к совершению неочевидных деяний (например, тщательно замаскированных, сопровождаемых четким распределением преступных ролей по заранее спланированной и отработанной схеме).

На наш взгляд, оперативно-розыскная характеристика преступлений имеет прикладное значение, которое является не только базисом для разработки рекомендаций по предупреждению, выявлению и раскрытию преступлений, но и самостоятельной научной категорией. Это явно прослеживается на примере криминалистических и оперативно-розыскных характеристик. Несмотря на общую функцию – борьбу с преступностью, они предназначены для разных субъектов – оперативного сотрудника и следователя. Каждый из них решает разные задачи, вытекающие из действующего законодательства, используя для этого специальные формы – следственные действия и оперативно-розыскные мероприятия, методы – исключительно гласные и как гласные, так и негласные, поэтому речь идет о самостоятельных видах правоохранительной деятельности – уголовно-процессуальной и оперативно-розыскной.

Кратко резюмируя изложенное, необходимо отметить, что главные различия данных характеристик проявляются в субъектах, которым они предназначены; решаемых ими задачах; формах и методах, которыми они могут реализовываться.

Отдельного внимания заслуживает информационная составляющая оперативно-розыскной характеристики, что главным образом отличает ее от других характеристик, исследуемых юридическими науками. Как верно отмечают И.И. Басецкий и В.Ч. Родевич, оперативно-розыскная характеристика преступлений – это совокупность гласной и негласной информации. В связи с этим рассматриваемая категория включает в себя самостоятельный и более широкий спектр сведений, не имеющий отношения к уголовному праву, криминологии, психологии, криминалистике и т. д.

Таким образом, оперативно-розыскная характеристика преступлений – это систематизированная информационная модель, состоящая из коррелирующих между собой структурных элементов, наполненных сведениями, полученными из гласных и негласных источников, которые позволяют в совокупности описать механизм совершения общественно опасных деяний для эффективной разработки практических рекомендаций по их предупреждению, выявлению и пресечению, представленных алгоритмом действий оперативного сотрудника.

Как показывает анализ научных трудов по исследуемой проблеме, ученые не едины во мнении о структуре оперативно-розыскной характеристики преступлений. Главная причина этого кроется в особенностях познания, осуществляемого с прикладной целью на примере отдельных видов общественно опасных деяний, которым свойственна разная структура, поскольку в одном случае то или иное звено играет важную роль, а в другом – оно и вовсе может отсутствовать.

В большинстве случаев исследователи включают в оперативно-розыскную характеристику преступлений сведения, описывающие уголовно-правовые признаки конкретного вида общественно опасного деяния; личность преступника; мотивацию криминального поведения; способ совершения преступления; предмет преступления; обстановку преступления; место совершения преступления; поведение жертвы преступления. Исходя из этого общая структура указанной характеристики выглядит достаточно разнообразной.

Однако наиболее целесообразно, как мы полагаем, при формировании оперативно-розыскной характеристики преступлений исходить прежде всего из объективных закономерностей включения тех или иных элементов, обладающих наибольшим информационным содержанием для решения задач, стоящих перед оперативным сотрудником. В данном аспекте разделяем утверждение С.Н. Князева, что в системе главное – не элементы, а взаимосвязи между ними, их взаимодействие, взаимоотношения. Аналогичной позиции придерживается и А.Е. Гучок, отмечая, что важнейшую роль в функционировании и развитии преступления играют системообразующие связи, благодаря которым все элементы его материальной структуры оказываются связанными воедино.

Таким образом, искусственное наполнение произвольными сведениями рассматриваемой характеристики недопустимо, так как подобное заведомо ведет к ее расширению и не позволяет выявить зависимости в структурных компонентах.

УДК 343.4

С.А. Черняк

О ПРОФИЛАКТИКЕ КИБЕРПРЕСТУПНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Согласно Концепции информационной безопасности Республики Беларусь целью обеспечения информационной безопасности является достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие.

В отечественных и зарубежных криминологических стратегиях борьбы с преступностью ведущее место отводится профилактике. Для такого вида противоправных деяний, как киберпреступность, профилактика имеет первостепенное значение.

На территории Республики Беларусь в последние годы преобладает тенденция совершения киберпреступлений в отношении жителей страны лицами из-за ее пределов, преимущественно с территории Украины и Российской Федерации. При этом имеющиеся правовые механизмы получения информации с использованием возможностей правоохранительных органов других государств не позволяют своевременно и в полном объеме получать необходимые сведения, что вызывает объективные трудности по установлению личности преступника и привлечению его к ответственности в соответствии с законодательством Республики Беларусь.

В деле противодействия киберпреступности и обеспечения информационной безопасности успех приносит только комплексный подход. В теории и на практике выделяют три основные группы мер профилактики, которые в совокупности образуют систему борьбы с данным явлением: правовые; организационно-управленческие; технические.

Правовые меры обеспечивают условия создания и поддержания системы информационной безопасности на должном уровне. К данной группе мер профилактики прежде всего относят нормы законодательства, устанавливающие уголовную ответственность за противоправные деяния в компьютерной сфере.

Кроме того, важнейшим на законодательном уровне является создание механизма, позволяющего согласовать процесс разработки законов с реалиями времени и прогрессом информационно-коммуникационных технологий.

Вместе с тем одними правовыми мерами сдерживания не всегда удается достичь желаемого результата. Становится очевидной необходимость использования организационно-управленческих мер предупреждения компьютерной преступности, таких как сохранение конфиденциальности информации; обеспечение правового режима информации как объекта собственности; предотвращение несанкционированных действий по отношению к информации, информационным ресурсам и системам; обеспечение прав субъектов в информационных процессах и др.

Помимо правовых и организационно-управленческих мер существенную роль в борьбе с киберпреступностью играют и меры технического характера. Среди таких мер можно выделить две группы – аппаратные и программные. Аппаратные меры предназначены для защиты компьютерной техники от нежелательных физических воздействий и закрытия возможных каналов утечки конфиденциальной информации. Программные меры защиты предназначены для непосредственной защиты информации.

В ходе реализации вышеуказанной системы мер по предупреждению киберпреступности в практической деятельности не все так однозначно. При проведении профилактической работы с населением и представителями государственного и частного секторов экономики обнаруживается ряд проблемных вопросов.

Несмотря на рост киберпреступности, в последние годы только относительно недавно принят ряд кардинальных мер по их предупреждению – в 2019 г. утверждена Концепция информационной безопасности Республики Беларусь; в 2020 г. в системе МВД Республики Беларусь проведены организационно-штатные мероприятия по дальнейшему развитию и совершенствованию подразделений по борьбе с киберпреступностью; в 2021 г. внесены уже давно назревшие изменения в гл. 31 Уголовного кодекса Республики Беларусь (УК); утвержден комплексный план мероприятий, направленных на принятие эффективных мер по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения на 2021–2022 гг.

Как показывает практика, самым слабым звеном в механизме совершения высокотехнологичных преступлений нередко оказывается человек. Проведенный управлением по противодействию киберпреступности криминальной милиции УВД Гродненского облисполкома за девять месяцев 2021 г. мониторинг категорий лиц, потерпевших от хищения имущества путем модификации компьютерной информации (ст. 212 УК), показал, что 27,8 % составляют лица рабочих специальностей со средним специальным образованием; 13,6 % – лица пенсионного возраста; 12,1 % – педагоги и учащиеся; 8,5 % – неработающие; 6,6 % – специалисты различных сфер с высшим образованием; 7 % – лица, находящиеся в декретном отпуске; 6 % – врачи и медперсонал; 2,9 % – работники торговли; 3,2 % – бухгалтеры и финансисты; 1,8 % – индивидуальные предприниматели и ремесленники; 1,8 % – правоохранители и военнослужащие; 8 % – иные категории.

Результаты проводимой профилактической работы с обучающимися, а также с родителями школьников показывают, что в настоящее время в подавляющем большинстве родители не выполняют обязанности по воспитанию детей в части привития им правил цифровой гигиены и поведения в виртуальном пространстве. Отчасти такое положение дел сложилось из-за того, что сами родители в силу различных причин не владеют данным инструментарием и не способны обучать подрастающее поколение.

Кроме того, учебные программы учреждений образования требуют коррекции с учетом внедрения в жизнь общества и развития информационно-коммуникационных технологий. Например, в ходе изучения предмета «Информатика», преподаваемого только в старших классах, совсем мало времени отведено изучению вопросов безопасного использования компьютерной техники и ответственности за совершение противоправных деяний. При этом учащиеся начинают использовать различную компьютерную технику, в том числе имеющую подключение к сети Интернет, уже в младшем школьном возрасте.

Видится необходимым в общеобразовательных учреждениях ввести соответствующие программы или спецкурсы в рамках курса «Информатика» для проведения комплекса мероприятий по разъяснению подросткам повышенной социальной опасности киберпреступлений, ознакомлению с уголовной ответственностью и наказаниями за их совершение.

Не меньше проблем возникает при взаимодействии с предприятиями и организациями различных форм собственности по вопросам принятия ими мер по обеспечению должного уровня информационной безопасности, правового просвещения и обучения персонала, разъяснению технологии безопасного хранения и обработки информации, формированию навыков безопасного поведения пользователей, имеющих доступ к информационным ресурсам предприятий.

На многих предприятиях не уделяют должного внимания этому вопросу, отсутствуют в штате соответствующие специалисты, руководство, в том числе и частных предприятий, не готово тратить дополнительные финансовые и временные ресурсы на проведение такой работы.

В то же время потенциальный преступник должен осознавать высокую вероятность быть обнаруженным и понести наказание за свои действия, поэтому важным элементом предупреждения киберпреступлений является проведение целевых мероприятий и распространение информации об успешной борьбе с преступностью в данной сфере, а также доведение гражданам информации о наиболее типичных способах совершения высокотехнологичных преступлений с целью принятия ими мер по предотвращению совершения в отношении их аналогичных преступлений.

УДК 343.985

А.М. Шинкевич

О СОДЕРЖАНИИ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ «ПРОВЕРОЧНАЯ ЗАКУПКА», «ОПЕРАТИВНЫЙ ЭКСПЕРИМЕНТ» И «КОНТРОЛИРУЕМАЯ ПОСТАВКА»

Оперативно-розыскная деятельность (ОРД) играет важнейшую роль в обнаружении и раскрытии преступлений. ОРД осуществляется с применением оперативно-розыскных мероприятий (ОРМ), которые на законодательном уровне в Республике Беларусь регулируются с 1992 г. Наиболее сложными ОРМ, на наш взгляд, являются «проверочная закупка», «оперативный эксперимент» и «контролируемая поставка». Это вполне естественно, ведь они требуют тщательной подготовки, привлечения вспомогательных сил органов, осуществляющих ОРД, технического сопровождения, проводятся в рамках дел оперативного учета и нуждаются в вынесении постановления (ст. 19 Закона от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» (далее – Закон об ОРД)).

По мнению законодателя, проверочная закупка представляет собой приобретение без цели потребления или сбыта у гражданина, организации предметов и документов, компьютерной информации и иных сведений или осуществление заказа на выполнение работ (оказание услуг) в целях получения сведений, необходимых для выполнения задач ОРД, т. е. по содержанию проверочная закупка представляет собой сделку, предметом которой выступают товары, работы или услуги, где в роли покупателя выступает лицо, действующее в интересах органов, осуществляющих ОРД. Как правило, такая сделка не является гражданско-правовой и носит противоправный характер, может быть заключена с лицом, персональные данные которого неизвестны. При этом законодатель ограничил предмет такой сделки, т. е. заказ запрещенных уголовным законом работ (услуг) предписано осуществлять в рамках оперативного эксперимента (ст. 28 Закона об ОРД).

Если обратиться к законодательному определению оперативного эксперимента, то можно отметить, что он определяется через созданную органом, осуществляющим ОРД, обстановку, максимально приближенную к предполагаемой преступной деятельности вовлекаемого в нее гражданина (граждан) (ст. 34 Закона об ОРД). Целью указанного мероприятия является вызывание определенного события, а также получение сведений, необходимых для выполнения задач ОРД. При этом законодателем не определено, о каком событии идет речь, а задачи ОРД (ст. 3 Закона об ОРД) весьма разнообразны, чтобы по всем проводить оперативный эксперимент. Складывающаяся практика проведения оперативного эксперимента свидетельствует, что целью его проведения, как правило, является задержание лица или нескольких лиц с поличным за совершение одного или нескольких взаимосвязанных преступлений.

В отличие от проверочной закупки при проведении оперативного эксперимента законодатель внес дополнительные ограничения, которые закрепил в качестве обязательных условий. В частности, при выявлении менее тяжкого, тяжкого и особо тяжкого преступления требуется заявление лица о преступлении, подготавливаемом, совершаемом или совершенном в отношении его или его близких, при условии его участия в указанном ОРМ (ст. 34 Закона об ОРД). Фактически в процессе оперативного эксперимента осуществляется документирование противоправной сделки, где в качестве заказчика выступает заявитель, принимающий участие в ОРМ, а исполнителя – лицо, чьи действия носят преступный характер.

Наиболее часто оперативный эксперимент с участием заявителя проводится в отношении конкретного должностного лица или группы лиц для выявления взяточничества.

При выявлении тяжкого или особо тяжкого преступления оперативный эксперимент может проводиться и без заявления в отношении неустановленного лица или группы лиц при условии предварительно проверенных органом, осуществляющим ОРД, сведений о признаках подготавливаемого, совершаемого или совершенного преступления. В большинстве своем оперативный эксперимент в отношении неустановленных лиц проводится для выявления преступлений, связанных с распространением наркотических средств, психотропных веществ, их прекурсоров или аналогов посредством использования сети Интернет.

С точки зрения законодателя, контролируемая поставка состоит в перемещении гражданином, организацией предметов и документов под контролем должностного лица органа, осуществляющего ОРД, т. е. речь идет также о противоправной сделке по перемещению товаров, как правило, запрещенных или ограниченных к такому перемещению (ст. 29 Закона об ОРД).

Во всех случаях при проведении проверочной закупки, оперативного эксперимента или контролируемой поставки со стороны органов, осуществляющих ОРД, фактически проводится документирование противоправной сделки, предметом которой выступают товары, работы или услуги. Заказчиком при проведении проверочной закупки и оперативного эксперимента всегда выступают лица, действующие в интересах органов, осуществляющих ОРД, а исполнителем – предполагаемые преступники. При контролируемой поставке, наоборот, заказчиком выступают преступники, а исполнителем лица, действующие в интересах органов, осуществляющих ОРД. Как правило, целью заключаемых сделок (проверочной закупки, оперативного эксперимента и контролируемой поставки) должностных лиц органов, осуществляющих ОРД, является документирование субъективной и объективной сторон одного или нескольких взаимосвязанных преступлений, в том числе совершаемых неустановленными лицами. Реализуемые действия по выполнению условий этих сделок в основном имитируют противоправ-