вляющих розыск (следователей, работников органов дознания); б) противодействие путем оказания противоправного воздействия на лиц – носителей информации (свидетелей, потерпевших и др.); в) противодействие, оказываемое на материальные следы преступления [3, с. 9].

Классификация противодействия по субъектам не раскрывает всех форм, так как оно может выражаться такими действиями, как фальсификация, утаивание, подкуп, шантаж, клевета, угрозы, подготовка ложного алиби, инсценировка, уничтожение следов преступления, дача заведомо ложных показаний и др.

Принимая во внимание, что между гражданином, обладающим оперативно-значимой информацией, и оперативным сотрудником в ходе осуществления розыска лиц, пропавших без вести при криминальных обстоятельствах, происходит общение, а также учитывая те обстоятельства, что способы противодействия выделяются с позиции теории сокрытия информации, в которой оперативный сотрудник либо гражданин, оказывающий содействие на конфиденциальной основе органу, осуществляющему ОРД, являются основным объектом воздействия, представляет интерес классификация противодействия по типу коммуникаций. Иными словами, мы полагаем уместным придерживаться деления способов противодействия на активные и пассивные. Пассивные способы противодействия проявляются в умолчании, несообщении, отказе от дачи показаний, а активные в подаче заведомо ложного заявления, сообщения, заведомо ложных показаниях, самооговоре, вербальной инсценировке. Рассуждая об активных способах противодействия, следует помнить, что цель противодействия заключается в воспрепятствовании установлению истины, оно может проявиться также в воздействии на оперативного сотрудника, в том числе в виде шантажа. При этом степень противодействия может увеличиваться по нарастающей, вплоть до угроз и подкупа, приобретая наступательный, агрессивный и массированный характер.

В основе классификации способов противодействия могут лежать существующие типы коммуникаций, также необходимо обратить внимание на отсутствие искренности, выражающейся в невербальных проявлениях. Это асимметричность мимики, ее длительность, диссоциация между выражением глаз, мимикой лба, губ, окраской лица, дыханием, которые являются не чем иным, как имитацией эмоций человека.

Другие поведенческие признаки, коррелирующие с ложью, могут свидетельствовать о попытках отстранить себя от сообщения ложной информации с целью свести к минимуму общение. Подобная стратегия может выражаться в уклончивости ответов, избежании смотреть прямо в глаза, отклоненном положении тела и увеличении дистанции с собеседником, тем самым опрашиваемое лицо пытается отстраниться от ложной информации.

Большую часть информации человек воспринимает по невербальным каналам, а невербальные коммуникации оказывают воздействие на сознание оперативного сотрудника, усиливая или ослабляя его уверенность в причастности того или иного лица к событию преступления, необходимо знать признаки, которые позволяют оперативным сотрудникам подтвердить обоснованность выдвинутых версий, определиться с направлением оперативного поиска, оценить имеющуюся информацию, выявить существующие противоречия, изобличить в обмане и получить правдивые показания, выбрать тактические приемы проведения ОРМ, устранить причастность лица к совершенному преступлению.

Таким образом, с целью эффективного решения задач по розыску пропавших лиц оперативному сотруднику необходимо идентифицировать оказываемое противодействие, которое может быть не только на физическом, но и на интеллектуальном уровне, уметь нейтрализовать его, опираясь на специальные знания.

1. Букейханов П.Е. Розыск пропавших без вести : науч.-метод. пособие. М., 2006.

2. Мартыненко Р.Г. Коммуникативное противодействие расследованию: способы, выявление, преодоление : автореф. дис. … канд. юрид. наук : 12.00.09. Краснодар, 2004.

3. Петрова А.Н. Противодействие расследованию, криминалистические и иные меры его преодоления : автореф. дис. … канд. юрид. наук : 12.00.09. Волгоград, 2000.

УДК 343.985

А.А. Ковальчук

СТРУКТУРА И СОДЕРЖАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ, НЕОБХОДИМЫХ ДЛЯ ВЫЯВЛЕНИЯ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ РЕКВИЗИТОВ БАНКОВСКИХ ПЛАТЕЖНЫХ КАРТОЧЕК, И УСТАНОВЛЕНИЯ ЛИЦ, ИХ СОВЕРШИВШИХ

Противодействие преступности на современном этапе развития информационных технологий тесно связано с использованием передовых достижений научно-технического прогресса, что обусловливает необходимость применения специальных знаний из различных отраслей на-

уки и техники. Данное обстоятельство в особенности касается борьбы с высокотехнологичными преступлениями, к которым, безусловно, относятся хищения, совершаемые с использованием реквизитов банковских платежных карточек (БПК).

Определяя понятие «специальные знания», наиболее точной нам видится формулировка Г.И. Грамовича: «систематизированные научные знания, умения, навыки в определенной области человеческой деятельности (исключая знания в области материального и процессуального права), полученные в результате целенаправленной профессиональной подготовки и опыта работы, которые используются в целях собирания доказательственной и ориентирующей информации о преступлении, а также способствуют разработке технических средств и приемов работы с доказательствами» [1, с. 89].

Учитывая специфику и высокую степень латентности преступлений рассматриваемой категории, эффективность борьбы с ними во многом зависит от наличия у оперативных работников соответствующих специальных знаний, без которых выявление хищений, совершаемых с использованием реквизитов БПК, и установление лиц, их совершивших, будет весьма затруднительно, а иногда и вовсе невозможно. Подтверждением данной позиции является то, что противодействие указанным преступлениям составляет компетенцию непосредственно подразделений по раскрытию преступлений в сфере высоких технологий (РПСВТ).

Анализ литературы показал, что позиции ученых на содержание перечня специальных знаний, необходимых для осуществления борьбы с хищениями, совершаемыми с использованием реквизитов БПК, в определенной степени схожи, но не являются одинаковыми. Каждый автор в некоторой степени расширяет указанный перечень, обоснованно добавляя в него знания из различных отраслей науки и техники. Учитывая это, становится очевидно, что отдельно взятому человеку в рамках процесса познания охватить весь объем знаний, потребность в использовании которых возникает при тех или иных обстоятельствах, не представляется возможным. Поэтому, резюмируя взгляды исследователей, мы полагаем рациональным разделять специальные знания на две категории: первоочередные и второстепенные. Первую из указанных категорий должны составлять знания, используемые оперативным работником постоянно при осуществлении своих непосредственных обязанностей. Ко второй категории знаний следует относить применяемые время от времени в тех или иных оперативно-тактических ситуациях.

Определяя содержание первой группы, необходимо понимать, что основу профессиональной деятельности оперативных подразделений составляет получение оперативно значимой информации. Исходя из отмеченного, использование специальных знаний оперативным работником должно быть направлено на улучшение качества информационного обеспечения указанной деятельности. При этом важно также учитывать, что представители подразделений РПСВТ работают прежде всего с компьютерной информацией. Таким образом, по нашему мнению, эти сотрудники должны в первую очередь обладать знаниями о методах, приемах и особенностях обнаружения, фиксации, получения, передачи и хранения компьютерной информации.

Рассмотрим более подробно содержание вышеуказанных знаний. Нами уже отмечалось, что возможности сети Интернет активно используются кардерами для создания коммуникативных площадок – форумов, и осуществления своей преступной деятельности [2]. При этом информация, размещенная в глобальной сети, может быть как общедоступной, так и ограниченного характера. Учитывая указанное, а также опираясь на опыт, накопленный подразделениями РПСВТ, представляется возможным выделить следующие виды знаний, необходимых оперативным сотрудникам: о штатных возможностях и приемах работы с различными поисковыми системами; правилах и способах использования программного обеспечения, предназначенного для получения доступа к сети, осуществления поиска и анализа информации в «глубокой сети»[1] и «темной сети»[2] (например, «WebSite-Watcher», «Tor» и др.); об основах построения социальных сетей и кардерских интернет-форумов, особенностях размещения на них информации и обеспечения коммуникации пользователей.

Другой ситуацией, требующей применения специальных знаний, является необходимость работы с компьютерной информацией при возможности непосредственного доступа к какому-либо программно-техническому устройству злоумышленника. В данном случае сотрудник подразделения РПСВТ должен обладать знаниями: о функционировании различных операционных систем, особенностях и местах хранения информации, в том числе временной, служебной; программно-аппаратных методах и приемах поиска, восстановления интересующих сведений и файлов, а также обеспечения отсутствия следов своей деятельности.

[1] Глубокая сеть (от англ. «Deep Web») – множество веб-страниц сети Интернет, которые не индексируются (не обрабатываются) поисковыми системами. В глубокой сети находятся веб-страницы, не связанные гиперссылками с другими страницами, а также ресурсы, доступ к которым ограничен, например, паролем (частные форумы, частные сети и др.).

[2] Темная сеть (от англ. «Dark Web») – скрытая сеть, соединения которой устанавливаются только между доверенными участниками с использованием нестандартных протоколов и портов, посредством, как правило, специального программного обеспечения.

Мы убеждены, что к категории первоочередных специальных знаний, необходимых оперативным работникам для противодействия хищениям, совершаемым с использованием реквизитов БПК, следует относить знания в сфере устройства системы электронных платежей, эмиссии и обращения БПК. В случае реального кардинга сотрудник подразделения РПСВТ в первую очередь должен обладать знаниями о способах и особенностях изготовления и использования дубликата БПК; при виртуальном кардинге указанному сотруднику необходимы знания о механизмах функционирования различных электронных платежных систем и интернет-магазинов, а также правилах осуществления онлайн-платежей с использованием реквизитов БПК. Нам видится, что без применения указанных знаний установление обстоятельств, возможных способов совершения рассматриваемых преступлений, поиск следов и, соответственно, определение личности злоумышленников будет весьма затруднительным.

Обозначить окончательный перечень второй группы знаний не представляется возможным в силу некоторой случайности возникновения ситуаций, в которых может потребоваться их применение. Вместе с тем, учитывая специфику рассматриваемой категории преступлений, нелишними, как мы полагаем, для сотрудников подразделений РПСВТ будут любые знания в сфере устройства и функционирования средств компьютерной техники, различного рода программного обеспечения, в области информационной безопасности и др.

Практика показывает, что необходимость самостоятельного применения специальных знаний сотрудниками вышеназванных подразделений при выявлении хищений, совершаемых с использованием реквизитов БПК, и установлении лиц, их совершивших, возникает при осуществлении информационного обеспечения оперативного обслуживания сферы рассматриваемых преступлений, подготовке и проведении отдельных оперативно-розыскных мероприятий, исследовании изъятых в ходе оперативно-розыскных мероприятий средств компьютерной техники и носителей компьютерной информации.

Таким образом, представляется уместным заключить, что применение специальных знаний является одним из основополагающих аспектов борьбы с преступлениями рассматриваемой категории. В свою очередь процесс их получения сотрудниками подразделений РПСВТ должен быть перманентным и носить достаточно интенсивный характер, что обусловлено стремительностью научно-технического прогресса.

1. Грамович Г.И. О совершенствовании правового регулирования применения специальных знаний и научно-технических средств в расследовании преступлений // Проблемы криминалистики : сб. науч. тр. / под общ. ред. Г.Н. Мухина. Минск, 2003.

2. Ковальчук А.А. О применении возможностей сети Интернет при выявлении хищений, совершаемых с использованием реквизитов банковских платежных карточек, и установлении лиц, их совершивших // Актуальные вопросы оперативно-розыскной деятельности : тез. докл. респ. науч.-практ. конф., Минск, 2 июня 2017 г. / Акад. М-ва внутр. дел Респ. Беларусь ; ред.: А.Н. Тукало (отв. ред.) [и др.]. Минск, 2017.

УДК 004.056.5:343.9.024

Е.В. Лизогубенко

КИБЕРПРЕСТУПНОСТЬ – СОВРЕМЕННЫЙ ВЫЗОВ ПРАВООХРАНИТЕЛЬНЫМ ОРГАНАМ

Современное состояние развития телекоммуникационных, информационных и компьютерных технологий обусловливает появление и быстрое развитие общественных отношений в сфере их использования. Более того, информационные технологии и компьютерные сети сегодня представляют собой важную отрасль экономики, развитие которой выходит за пределы экономики одной страны и характеризуется наличием устойчивых международных связей.

Вместе с тем информационное пространство стало местом и в то же время непосредственно инструментом совершения преступлений. На сегодня преступление не требует предварительной обработки клиента и личного контакта с потенциальной жертвой. Главным инструментом преступника становится только компьютер и доступ к информационно-коммуникационным системам, где он с помощью компьютерных вирусов и других противозаконных технических средств получает доступ к базам данных, банковским счетам, автоматизированным системам управления.

Так, кражи данных платежных карт (банковских счетов) или данных доступа к системе Интернет-банкинга с целью завладения средствами клиентов банка, похищения персональных данных и коммерческой информации частных компьютеров или серверов, умышленное повреждение работы информационных систем или средств коммуникаций с целью создания убытков компаниям – это далеко не полный перечень возникших угроз, благодаря бурному развитию современных информационных технологий, и, соответственно, появилось такое понятие, как киберпреступность.