Первый аспект – способность найти общий язык с объектами, которые предрасположены к девиантному поведению, в частности с лицами, подготавливающими, совершающими или совершившими преступления. В этом случае с помощью данного качества оперативный сотрудник сможет посредством проведения разведывательного опроса или иных оперативно-розыскных мероприятий узнать оперативно значимую информацию, причем не только о преступлении, в котором замешан каким-либо образом данный объект, но и, возможно, о других противоправных деяниях и лицах, причастных к ним.

Второй аспект заключается в умении найти подход к коллегам, руководителям и иным субъектам, оказывающим содействие оперативному сотруднику. Благодаря данному содействию оперативный сотрудник может обеспечить себя любой дополнительной оперативно значимой информацией, например получение сведений от информационного центра Министерства внутренних дел Российской Федерации или от подразделения оперативно-розыскной информации.

Под наблюдательностью понимается способность оперативного сотрудника подмечать такие явления и факты, которые могут быть незаметны гражданским лицам. Данная особенность также напрямую влияет на результаты проведения оперативно-розыскных мероприятий. В частности, данное качество проявляется при проведении всех несанкционируемых оперативно-розыскных мероприятий: опроса, наведения справок, сбора образцов для сравнительного исследования, исследования предметов и документов и отождествление личности. Во время опроса оперативный сотрудник должен непосредственно наблюдать за изменениями мимики, движений тела, дыханием и другими изменениями девиантного субъекта. При сборе образцов для сравнительного исследования оперативный сотрудник может обнаружить иные предметы и документы, которые несут в себе оперативно значимую информацию для выявления и раскрытия преступления. В ходе исследования предметов и документов наблюдательностью должно обладать сведущее лицо, владеющее специальными знаниями в сфере, к которой относится данный предмет или документ. Отождествление личности может проводиться как оперативным сотрудником, так и опознающим лицом. В случае если отождествление личности проводится в искусственно созданных условиях, то оперативному сотруднику и опознающему лицу следует сосредоточить все усилия, так как время может быть ограничено. Таким образом, наблюдательность является одним из основных качеств оперативного сотрудника, так как в большей степени именно от него зависят положительные результаты проведения оперативно-розыскных мероприятий.

Быстрое реагирование на трансформацию оперативной обстановки также имеет прямую связь с результатами оперативно-розыскной деятельности. Посредством быстрого реагирования в экстремальной ситуации оперативного сотрудника можно внести координирующие изменения в порядок проведения оперативно-розыскного мероприятия, что может иметь решающие значение.

Психологическая устойчивость важна при всех аспектах служебной деятельности оперативных сотрудников. Работа оперативного сотрудника является одной из самых сложных по различным обстоятельствам. Ему приходится контактировать как с девиантными субъектами, так и с коллегами по службе, принимать важные решения самостоятельно, исходя их складывающейся оперативной обстановки. Для того чтобы находить общий язык со всеми субъектами, оперуполномоченный должен обладать психологической устойчивостью.

Хорошая память необходима на всех этапах оперативно-служебной деятельности, при проведении как несанкционируемых оперативно-розыскных мероприятий, так и ведомственного и судебного санкционирования. Оперуполномоченный должен запоминать большой объем информации при проведении мероприятий, в частности таких как опрос, отождествление личности, сбор образцов для сравнительного исследования, исследование предметов и документов и наведение справок.

Таким образом, в совокупности все вышеперечисленные характеристики личности складываются в образ хорошего, работоспособного сотрудника оперативного подразделения. Сотрудник, обладающий всеми вышеуказанными качествами, может с легкостью выполнять любые поставленные перед ним задачи.

УДК 343.37

О.В. Маркова

ПРЕСТУПЛЕНИЯ В ПЛАТЕЖНЫХ СИСТЕМАХ КАК УГРОЗА ФИНАНСОВОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Обеспечение финансовой безопасности государства невозможно без использования надежной платежной системы, как национальной, так и международной. Многомиллиардные переводы денежных средств по всему миру через платежные системы ежегодно увеличивают количество несанкционированных преступных операций, связанных с посягательствами на них.

В соответствии со ст. 25 Банковского кодекса Республики Беларусь одной из основных целей деятельности Национального банка является организация эффективного, надежного и безопасного функционирования платежной системы.

Платежная система чаще всего рассматривается в контексте институциональной ее составляющей и представляет собой совокупность самостоятельных организаций, которые взаимодействуют между собой по установленным правилам и процедурам по поводу перевода денежных средств. Речь идет о безналичных и электронных денежных средствах, перевод которых может осуществляться исключительно в платежной системе. Криптовалюта как средство платежа в виде кода, основанного на технологии блокчейн, используется в децентрализованных платежных системах, а значит, тоже может рассматриваться как платежное средство в платежной системе. Наличные деньги не являются объектом отношений в платежных системах, поскольку прием наличных денег и их обмен не зависят от оператора платежной системы, оператора услуг платежной инфраструктуры и участников платежной системы, они обязательны к приему на территории государства. Существуют, например, и игровые деньги (баллы, бонусы), которые используются участниками определенного игрового сообщества в виртуальном мире. Игровые деньги, заработанные в одной игре, невозможно потратить в другой, однако их приобретение часто

осуществляется за реальные деньги посредством использования электронных кошельков и банковских платежных карт. Так как игровые деньги носят ограничительный характер, они не относятся к платежным средствам в платежных системах.

Отношения, возникающие в платежной системе между ее участниками, – особая группа общественных отношений, охраняемых законом, в том числе мерами уголовно-правового воздействия. Платежная система как таковая может использоваться в преступных целях (финансирование терроризма, легализация (отмывание) преступных средств, незаконный оборот наркотических средств, дача или получение взятки), а могут иметь место нарушения отношений в самой платежной системе. Чаще всего действиями преступников вред причиняется отношениям, связанным с переводом денежных средств, эмиссией электронных средств платежа и платежных (расчетных) документов, обеспечением информационной безопасности участников платежных систем. Отдельной статьи в уголовном законодательстве, предусматривающем ответственность за преступные посягательства, связанные с использованием платежной системы, нет. Такие правонарушения относятся к имущественным преступлениям, преступлениям против порядка осуществления экономической деятельности, преступлениям против информационной безопасности. В зависимости от видового объекта преступного посягательства все преступления, совершаемые в платежных системах, можно разделить:

на преступления, посягающие на общественные отношения, обеспечивающие имущественные интересы участников платежных систем, предусмотренные ст. 205 (кража), ст. 209 (мошенничество) и ст. 212 (хищение путем использования компьютерной техники) УК Республики Беларусь;

преступление, посягающее на установленный порядок эмиссии платежных средств, предусмотренное ст. 222 (изготовление либо сбыт поддельных платежных средств) УК Республики Беларусь;

преступления, посягающие на безопасность компьютерной информации участников платежной системы, предусмотренные ст. 349 (несанкционированный доступ к компьютерной информации), ст. 352 (неправомерное завладение компьютерной информацией), ст. 353 (изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети), ст. 354 (разработка, использование либо распространение вредоносных программ), ст. 355 (нарушение правил эксплуатации компьютерной системы или сети) УК Республики Беларусь.

Преступники, совершая правонарушения в платежных системах, действуют скрытно и незаметно для потерпевших, поскольку перевод денежных средств осуществляется без участия законного держателя средства платежа. Используя удаленный доступ к банковскому счету или электронному кошельку, при помощи технических средств и специального программного обеспечения злоумышленники могут осуществлять несанкционированные финансовые операции из любой точки мира, имея лишь доступ к сети Интернет. Становятся распространенными случаи хищений криптовалюты с криптобирж, совершения хакерских атак на процессинговые центры операторов платежных систем.

Преступления, совершаемые с использованием платежных систем, представляют реальную угрозу финансовой безопасности государства, они являются латентными, высоко технически оснащенными, преступники умело маскируют следы несанкционированных операций и остаются неустановленными, причиняют колоссальный материальный ущерб всем участникам платежной системы. Имея доступ ко всем безналичным или электронным средствам, преступники могут похитить средства сверх лимита, который в реальности находится на счете потерпевшего (например, если держателю счета представляется банком возможность получения кредита или офердрафта). Остается и проблема обеспечения безопасности личных данных участников платежной системы, так как доступ ко многим идентифицирующим сведениям может быть использован преступниками в других преступных целях.

Перечисленные риски неправомерного использования платежной системы в преступных целях не только подрывают финансовую безопасность государства в целом, но и имеют негативные последствия для участников платежной системы в виде денежных убытков и подрыва деловой репутации банков и иных небанковских кредитно-финансовых организаций. Участники платежной системы должны постоянно оповещаться в случаях авторизации их данных или платежных инструментов, должна быть усилена финансовая ответственность банков за потери денежных средств со счетов клиентов в случаях, если клиенты не были проинформированы о совершении финансовой операции. В качестве одной из мер по предотвращению рассматриваемого вида преступления может быть наделение специальных государственных органов правом блокировки фишинговых сайтов и мошеннических колл-центров при поступлении соответствующих сообщений о совершении криминальных переводов денежных средств через платежные системы. Повышение информационной безопасности участников платежных систем, разработка средств защиты клиентов, двойная аутентификация (запрос PIN-кода и одноразового пароля, биометрическая система идентификации клиента), развитие специальных программ, позволяющих выявлять незаконные финансовые операции, совершенствование антивирусного программного обеспечения банковских приложений позволят минимизировать риски совершения преступлений в платежных системах.

УДК 343.13

М.К. Ниязов

ЗНАЧЕНИЕ ИЗМЕНЕНИЙ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В РЕСПУБЛИКЕ УЗБЕКИСТАН

Сложно представить себе работу правоохранительных органов без такой важной ее составляющей, как оперативно-розыскная деятельность. Законодательное закрепление оперативно-розыскной деятельности стало важным шагом в укреплении правоохранительной деятельности в Республике Узбекистан. В частности, Закон Республики Узбекистан № ЗРУ-344 «Об оперативно-розыскной деятельности» принят 25 декабря 2012 г. Сотрудники органов, осуществляющих ОРД, находятся