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

в состоянии постоянного анализа складывающейся криминально-криминогенной ситуации с целью обнаружения каких-либо сведений и признаков, свидетельствующих о подготовке, приготовлении или покушении на правонарушение, и недопущения общественно опасных последствий. Необходимость применения оперативно-розыскных мероприятий как негласных способов решения задач доказана временем, когда правоохранительные функции объективно не могут быть решены исключительно гласными формами деятельности. Вопросы изменения тактики, способов, средств, методов осуществления противоправной деятельности являются предметом научно-аналитической деятельности для последующего внесения коррективов во внутриведомственные акты и инициирования внесения изменений в действующее законодательство. Это взаимодействие должно быть постоянным, обеспечивать плотную взаимосвязь науки и практики правоприменительной деятельности.

Закон Республики Узбекистан № ЗРУ-651 «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан в связи с совершенствованием законодательства, направленного на охрану личных прав и свобод граждан» опубликован 1 декабря 2020 г.

Уголовно-процессуальный кодекс Республики Узбекистан принят в 1994 г. Законодатели и специалисты, участвовавшие в принятии Закона, на тот момент не могли предусмотреть стремительные изменения в развитии видов, способов связи и технических возможностей по передаче, перехвату и фиксации информации, руководствуясь лишь доступными на тот момент уровнем технического развития, известными видами, способами связи и их фиксации.

Если рассмотреть детально внесенные в УПК и Закон Республики Узбекистан от 25 декабря 1998 г. № 721-I «О гарантиях адвокатской деятельности и социальной защите адвокатов» изменения, то станет очевидным, что внесены незначительные поправки с учетом требований развития общества и научно-технического прогресса. Так, если ранее использовался термин «прослушивание переговоров, ведущихся с телефонов и других переговорных устройств», то в настоящее время он заменен на более емкое и охватывающее современные тенденции понятие «прослушивание переговоров, ведущихся с телефонов и других телекоммуникационных устройств, снятие передаваемой по ним информации». Это обусловлено тем, что при совершении многих особо опасных преступлений используются телекоммуникационные устройства и передаваемая по ним информация (социальные сети, мессенджеры). Использование возможностей данного вида ОРМ дает возможность правоохранительным органам своевременно обнаруживать, пресекать противоправные действия и, что немаловажно, использовать полученные в ходе ОРМ данные в качестве доказательств по уголовному делу.

Кроме того, изменения, внесенные в УПК, затронули субъекта, осуществляющего прослушивание переговоров, ведущихся с телефонов и других телекоммуникационных устройств. Если ранее в УПК в качестве единственного органа, исполнявшего постановления о проведении прослушивания, значились органы Службы государственной безопасности, то теперь им стал уже обезличенный «специально уполномоченный государственный орган». По законодательству органом, осуществляющим исполнение таких видов ОРМ, может быть как один, так и несколько уполномоченных органов. Законодательного ограничения не имеется.

Эра магнитных лент осталась в далеком прошлом, на смену им пришли более качественные, современные и устойчивые к внешним воздействиям цифровые записи, в связи с чем в ст. 170 УПК в части фиксации в ходе прослушивания переговоров и приобщения к протоколу следственного действия слова «магнитная лента с фонограммами переговоров» были заменены на слова «зафиксированная информация» или «запись переговоров».

Важным изменением, внесенным в ст. 382 УПК, стало также предоставление органам, осуществляющим доследственную проверку, возможностей по использованию ОРМ, ограничивающих права на неприкосновенность жилища, тайну переписки, телефонных и иных переговоров, почтовых, курьерских отправлений и телеграфных сообщений, передаваемых по каналам связи, санкционируемых прокурором. Если ранее данное право было только у органов, наделенных правом проведения дознания и предварительного следствия, то теперь ходатайствовать о применении ОРМ вправе и органы, осуществляющие доследственную проверку, что предоставляет еще одну действенную возможность в борьбе с преступностью.

Внесены также важные изменения в Закон Республики Узбекистан «Об оперативно-розыскной деятельности». Ст. 14 Закона предусматривала возможность проведения 16 ОРМ. Внесенными изменениями были объединены самостоятельные виды оперативно-розыскных мероприятий в одно ОРМ, а именно прослушивание переговоров, ведущихся с телефонов и других переговорных устройств, а также снятие информации с технических каналов связи. ОРМ также дополнены новым видом – получение информации о соединении между абонентами или абонентскими устройствами, которое заключается в получении информации о дате, времени, продолжительности и других сведений о соединении между абонентами или абонентскими устройствами. Кроме того, определенные изменения претерпел еще один вид ОРМ – обследование жилых и иных помещений, зданий, сооружений, участков местности и транспортных средств, в ходе которого стало возможным проведение осмотра и изучение технических средств (компьютеров и устройств связи), что также преследует цель обеспечения полноты и всесторонности проводимого оперативно-розыскного мероприятия.

Следует отметить, что ранее Законом «Об оперативно-розыскной деятельности» было определено, что перечень дел оперативно-розыскного производства и порядок их ведения устанавливаются законодательством, что было затруднительно в связи с необходимостью сохранения конфиденциальности данных сведений. Теперь внесенные в ч. 3 ст. 18 Закона изменения позволяют защищать такую сугубо профессиональную информацию, как ведение дел оперативно-розыскного производства.

Закон «Об оперативно-розыскной деятельности» также дополнен ст. 28^1, допускающей международное сотрудничество в сфере оперативно-розыскной деятельности, что дает дополнительный импульс к взаимодействию и сотрудничеству в соответствии с международными договорами.

Анализ внесенных изменений позволяет констатировать, что, исходя из требований времени и практики использования ОРМ, произошла их корректировка в соответствии с государственным, общественным развитием и требованиями времени. Данная взаимосвязь законодательного закрепления ОРД и ее реализации на практике является естественным и необходимым для эффективной борьбы с преступностью и обеспечения надежной защиты прав, свобод и законных интересов граждан.