в ходе проведения оперативно-розыскных мероприятий информацию, содержащую данные о событиях и действиях, создающих угрозу национальной безопасности Республики Беларусь, подготавливаемых, совершаемых либо совершенных правонарушениях, повлекших либо способных повлечь за собой причинение вреда охраняемым законодательством интересам граждан Республики Беларусь, иностранных граждан, лиц без гражданства, организаций, общества и государства, и требующую принятия мер реагирования.

Указанные сведения могут использоваться органами, осуществляющими ОРД (ст. 12 Закона об ОРД), в целях профилактики правонарушений после представления данных материалов в порядке, определенном законодательством, в орган уголовного преследования для подготовки и проведения следственных и иных процессуальных действий, доказывания в уголовном процессе.

В проекте постановления необходимо закрепить положение о том, что решение о направлении сведений, содержащихся в материалах ОРД, в целях профилактики правонарушений принимается должностным лицом органа, осуществляющего ОРД. Перечень должностных лиц, уполномоченных на принятие решений о направлении сведений, содержащихся в материалах ОРД, в целях профилактики правонарушений должен определяться Министерством внутренних дел, Комитетом государственной безопасности, Государственным пограничным комитетом, Службой безопасности Президента Республики Беларусь, Оперативно-аналитическим центром при Президенте Республики Беларусь, Комитетом государственного контроля, Государственным таможенным комитетом, Министерством обороны.

В целях четкого определения и законодательного закрепления организационно-правовых аспектов по данному направлению служебной деятельности необходимо также рассмотреть вопрос о компетенции должностного лица органа, осуществляющего ОРД, и закрепить в проекте постановления следующие положения.

Приняв решение о направлении содержащихся в материалах ОРД сведений в целях профилактики правонарушений, должностное лицо органа, осуществляющего ОРД: выносит постановление о направлении сведений, содержащихся в материалах ОРД, с указанием в нем перечня оперативно-служебных документов, содержащих направляемые сведения, лица, в отношении которого они направляются, а также адресата (постановление помещается в дело оперативного учета либо номенклатурное дело или иное дело); осуществляет подготовку и направление информационного письма (без ограничительного грифа) с отражением в нем сведений, содержащихся в материалах ОРД.

Необходимо также рассмотреть вопросы (и закрепить в проекте постановления):

о порядке направления информационных писем (в соответствии с компетенцией), в том числе о запрещении в этих письмах указывать порядок проведения оперативно-розыскных мероприятий, тактику и методику их осуществления, ссылки на конкретные материалы ОРД, иные данные, содержание которых может привести к разглашению сведений, составляющих государственные секреты;

круге руководителей, которым направляются данные письма (в том числе руководителям субъектов хозяйствования).

С целью соблюдения конституционных прав и свобод граждан целесообразно закрепить в данном проекте постановления положение о том, что сведения, указанные в информационных письмах, не являются основанием для ограничения прав, свобод и законных интересов граждан и (или) юридических лиц, а также основанием для привлечения граждан и (или) юридических лиц к установленной законодательством ответственности. При получении этих писем руководители (их заместители) ведомств и субъектов хозяйствования могут (и должны) учитывать указанные сведения при решении вопросов кадровых назначений в отношении этих лиц, в том числе при оценке эффективности выполнения данными работниками должностных (функциональных) обязанностей, соответствия их морально-деловым качествам по занимаемой должности и т. д.

Таким образом, подготовка данного проекта постановления позволит грамотно и своевременно на законодательном уровне устранить имеющийся в настоящее время правовой пробел в ОРД в связи с дополнением в 2021 г. ст. 49 Закона об ОРД частью четвертой.

УДК 343.935

А.В. Вальтер

ДИСТАНЦИОННОЕ МОШЕННИЧЕСТВО: НЕКОТОРЫЕ ОСОБЕННОСТИ ПРЕСТУПЛЕНИЙ И АКТУАЛЬНЫЕ ВОПРОСЫ СБОРА ИНФОРМАЦИИ, ИМЕЮЩЕЙ ДОКАЗАТЕЛЬСТВЕННОЕ ЗНАЧЕНИЕ, НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ РАССЛЕДОВАНИЯ УГОЛОВНОГО ДЕЛА

В связи с развитием информационных технологий в настоящее время происходит рост количества поступающих спам-звонков с использованием IP-телефонии, СМС-рассылки различного содержания на теле-

фонные номера граждан Российской Федерации и Республики Беларусь, целью которых, как правило, является совершение дистанционного мошенничества.

Явление дистанционного мошенничества сегодня приобретает масштабы накатывающейся волны. Преступники, находясь на удалении от жертвы, совершают противоправные действия, отрабатывают различные методы социальной инженерии и совершенствуют свои навыки по удаленному хищению безналичных денежных средств, оставаясь нередко вне поля зрения правоохранительных органов.

В судебной практике Российской Федерации при постановлении обвинительных приговоров по фактам мошеннических действий с использованием информационных технологий все чаще используются термины «дистанционное мошенничество» либо «мошенничество, совершенное дистанционным способом». Однако в настоящее время единого подхода к определению термина «дистанционное мошенничество» в уголовно-правовой доктрине как Республики Беларусь, так и Российской Федерации не выработано.

С учетом способов совершения мошеннических действий с использованием информационных технологий в ситуации удаленного нахождения злоумышленника под дистанционным мошенничеством мы понимаем хищение безналичных денежных средств и (или) электронных денежных средств с использованием электронных средств платежа и технологий обмана информационно-телекоммуникационным или телефонным способом.

В уголовном законодательстве Республики Беларусь уголовно-правовая норма, в диспозиции которой предусмотрены основания для привлечения к уголовной ответственности за дистанционное мошенничество, содержатся в ст. 209 «Мошенничество» УК, в Российской Федерации – ст. 159, 159.3 и 159.6 УК.

Дистанционное мошенничество, как правило, совершается с использованием различных технических средств, имеющих доступ к интернету и сотовой связи. Так, злоумышленники в ходе совершения преступления могут применять мобильные телефоны, смартфоны, планшетные компьютеры, стационарные компьютеры и другие компьютерные устройства.

Необходимо отметить, что следователь либо дознаватель имеет возможность, обратившись к общедоступным базам данных, установить первоначальную информацию, необходимую для дальнейшего производства по уголовному делу на первоначальном этапе предварительного расследования, используя информацию об операторах сотовой связи,

интернет-услуг, организациях, предоставляющих услуги IP-телефонии, доменных имен, хостингов и др.

Рассмотрим распространенный способ дистанционного мошенничества, когда на телефон потерпевшего поступает телефонный спам-звонок в целях получения конфиденциальной информации о банковском счете и похищения денежных средств с его банковского счета.

С целью сокращения времени, необходимого для производства по уголовному делу на первоначальном этапе предварительного расследования, и с учетом соблюдения разумных сроков уголовного судопроизводства для установления первоначальной информации, имеющей доказательственное значение по уголовному делу, следователь (дознаватель) может инициативно истребовать у потерпевшего выписку о движении безналичных денежных средств по его банковскому счету и установить, куда они были перечислены с его счета. В кратчайшие сроки потерпевший также может инициативно по указанию должностного лица, производящего предварительное расследование, получить информацию от оператора связи о телефонных соединениях со злоумышленником.

При этом необходимо отметить ряд технических сложностей, возникающих при расследовании данной категории дел, которые следователь (дознаватель) не имеет возможности решить самостоятельно в сжатые сроки:

проведение оперативно-розыскных мероприятий в рамках оперативно-розыскной деятельности по установлению организаций, оказывающих злоумышленникам услуги IP-телефонии (Voice over IP-телефонии) и искусственного изменения входящего номера телефона (спуфинг);

установление местонахождения подозреваемого в случае использования VPN-шифрования каналов интернет-связи;

усложненная процедура получения личной информации об абоненте по номеру международного идентификатора (IMEI) мобильного устройства с учетом необходимости соблюдения конституционных прав и свобод граждан;

вопросы оперативной блокировки банковских счетов и банковских карт с учетом необходимости получения судебного разрешения на указанную операцию.

Несмотря на имеющиеся сложности, следователь (дознаватель) имеет возможность самостоятельно установить предварительную информацию об актуальном операторе связи, смене оператора связи, абонентском номере телефона звонящего, устройстве для звонков (телефон, планшет, компьютер и т. д.) путем использования программных средств, представленных на интернет-сайтах: www.zniis.ru; www.htmlweb.ru и др. После чего направить запросы актуальным операторам связи, предоставляющим в том числе услуги IP-телефонии злоумышленникам,

использующим средства связи для совершения дистанционного мошенничества.

Следует также отметить ситуации дистанционного мошенничества с использованием интернет-соединений, когда необходимо установить IP-адрес точки выхода в интернет, с которой подозреваемый в преступлении совершал противоправные действия. В такой ситуации возможно использование информации с сайта https://who.is/, с использованием которого в случае имеющегося IP-адреса или наименования домена (сайта) можно получить контакты администрации организации, зарегистрировавшей домен злоумышленника, и отправить ей запрос о представлении соответствующей информации о клиенте.

При этом должностным лицам, производящим предварительное расследование, необходимо отслеживать вопросы, связанные с оплатой злоумышленником услуги интернет-связи, обслуживания домена, хостинга (хранилища), где размещена информация, непосредственно отображенная на интернет-сайте, с оплатой услуг сотовой связи. Так, подозреваемое лицо, используя VPN-шифрование в ходе совершения мошеннических действий, может допустить просчет и произвести оплату за услуги со своей личной банковской платежной карты либо карты своего знакомого, родственника и др. Таким образом, помимо запроса о представлении общей информации об установочных данных злоумышленника у оператора связи (интернет-, сотовая связь и т. д.), интернет-услуг (VPN, IP-телефония и т. д.), необходимо получить информацию обо всех платежах, произведенных злоумышленником (данные банковского счета, банковской платежной карты, IP-адрес, с которого производился платеж, наименование интернет-кошелька, его номер, какой криптовалютой совершен расчет и т. д.).

С учетом участившихся случаев использования криптовалют в ходе осуществления противоправной деятельности следует отметить создание на базе Федеральной службы по финансовому мониторингу программного средства «Прозрачный блокчейн», которое положительно зарекомендовало себя и было использовано при раскрытии ряда резонансных преступлений.

В заключение отметим, что приведенные нами примеры – это лишь часть имеющейся проблемы по раскрытию фактов дистанционного мошенничества, связанной с установлением цифровых следов преступной деятельности злоумышленников, так как в дальнейшем могут появиться сложности в рамках международного взаимодействия – длительный обмен информацией с учетом международных соглашений, ряд других зарегулированных бюрократических моментов, которые могут возникнуть в случае международной координации преступниками своей противоправной деятельности.

УДК 343.985

В.М. Веремеенко, В.В. Кравец

ОБЕСПЕЧЕНИЕ КОНСТИТУЦИОННЫХ ПРАВ И СВОБОД ЧЕЛОВЕКА И ГРАЖДАНИНА ПРИ ПРОВЕДЕНИИ ОПЕРАТИВНОГО ЭКСПЕРИМЕНТА

В соответствии со ст. 2 Конституции Республики Беларусь человек, его права, свободы и гарантии их реализации являются высшей ценностью и целью общества и государства.

Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства. Вместе с тем, защищая человека от преступных посягательств, государство в лице правоохранительных органов нередко вынужденно вторгается в личную жизнь граждан, которые тем или иным образом причастны к совершению преступления. Такая деятельность государства регламентирована ст. 23 Конституции Республики Беларусь, в которой закреплено, что ограничение прав и свобод личности допускается только в случаях, предусмотренных законом, в интересах национальной безопасности, общественного порядка, защиты нравственности, здоровья населения, прав и свобод других лиц.

Одним из видов деятельности правоохранительных органов является оперативно-розыскная деятельность, которая регламентируется Законом Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» (далее – Закон об ОРД). По нашему мнению, наиболее ярко проблема обеспечения прав и свобод человека и гражданина выражена именно в этом виде правоохранительной деятельности, как специфической форме борьбы с преступностью. Это обусловлено тем, что ОРМ могут проводиться в негласном порядке, что связано с дополнительными рисками по неправомерному вторжению в права человека.

На наш взгляд, одним из дискуссионных ОРМ является оперативный эксперимент, поскольку при его проведении возникает ряд проблем разграничения с таким противоправным деянием, как подстрекательство к преступлению.

В Законе об ОРД закреплены основания и условия для проведения оперативного эксперимента:

наличие заявления, сообщения гражданина о подготавливаемом, совершаемом или совершенном в отношении его или его близких менее тяжком, тяжком или особо тяжком преступлении – при условии участия в оперативном эксперименте гражданина, в отношении которого готовится, совершается или совершено преступление;

наличие предварительно проверенных органом, осуществляющим оперативно-розыскную деятельность, сведений о признаках подготав-