способах подготовки, совершения и сокрытия дистанционного мошенничества (способы обмана потерпевших, приемы манипуляций их сознанием и поведением);

особенностях личности преступника;

информационно-коммуникационной среде как сфере возникновения информации о совершении дистанционных мошенничеств;

механизме образования следов как источников информации о дистанционных мошенничествах;

видах электронных носителей информации об обстоятельствах дистанционных мошенничеств.

Задача исследователей – наполнение каждого из элементов ОРХ дистанционного мошенничества своим содержанием на основе изучения материалов оперативно-следственной и судебной практики.

УДК 343.98

В.М. Данатарова

СОВРЕМЕННЫЕ СПОСОБЫ СОВЕРШЕНИЯ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОЙ СВЯЗИ

В связи с интенсивным развитием средств мобильной связи, технологическими прорывами в сфере мобильных гаджетов, а также в связи с формированием привязанности к ним возрастает количество мошенничеств, совершенных с их использованием.

Изучая научные работы, посвященные мошенничеству с использованием мобильной связи, мы приходим к выводу, что исследования в данном направлении практически отсутствуют или имеют поверхностный характер.

В большинстве научных работ описаны основные виды мошенничества: «получите выигрыш», «нигерийские письма», «ваш родственник в полиции», «ошибочное пополнение мобильного счета», «звонок из банка» и т. п. Они уже являются достаточно изученными со стороны ученых, не вызывают у практиков трудностей в их раскрытии и используются преступниками крайне редко.

Мы считаем, что необходимо уделить внимание относительно новым видам мошенничества и рассмотреть их способы совершения, с которыми на сегодняшний день сталкиваются и испытывают трудности сотрудники подразделений по борьбе с киберпреступностью МВД Украины.

Так, одним из современных способов завладения денежными средствами жертвы является SMS-фишинг. В декабре 2020 г. одним из фи-

нансовых учреждений Украины были зафиксированы рассылки фишинговых SMS-сообщений с использованием поддельных альфа-имен банков. Прежде всего стоит разобраться, что же такое альфа-имя. Согласно информации указанной в словаре терминов, альфанумерическое имя, или альфа-имя, – 11 символов в строке отправителя SMS. В нем указывается название компании или бренда, но не номер мобильного телефона. Например, банковское учреждение «Кредобанк» при SMS-рассылке использует альфа-имя KREDOBANK (состоит из больших букв латиницы). Мошенники подделывают такие альфа-имена банков, чтобы вызвать доверие у клиентов финансовых учреждений.

Используя поддельное альфа-имя, мошенники совершают рассылку сообщений, в которых описаны вымышленные проблемы с платежной картой потенциальной жертвы (блокировка платежной карты, кража данных платежной карты и т. п.) и одним из способов решения проблемы предлагается немедленно связаться с сотрудником банка и следовать его указаниям. Целью такого SMS-сообщения является создание информационно-психологического влияния для умышленного введения пользователя в заблуждение. Находясь в состоянии стресса, взволнованная жертва следует указаниям лже-сотрудника банка – совершает выведение денежных средств путем перечисления на «безопасный» счет, уже якобы открытый учреждением на имя клиента. Таким образом, потерпевший, находясь под влиянием мошенника, с целью защиты своих денежных средств выполняет манипуляции по перечислению денег прямо на счет преступника.

Мошенники, использующие SMS-фишинг, могут представляться сотрудниками банков, сервисных компаний или компаний-операторов лотерей. Как показывает практика, аргументы в их арсенале могут быть разные, но задача состоит в том, чтобы непосредственно выманить денежные средства и получить доступ к управлению текущим счетом.

Сходным способом пользуются преступники и для создания условий кражи авторизационных данных для доступа к системам дистанционного банковского обслуживания (онлайн-банкинга) и платежных карточек. Но стоит отметить, что в этом случае денежные средства похищаются втайне от потерпевшего. Посему имеет место квалификация такого преступления как кража (тайное хищение чужого имущества).

Следующим способом совершения мошенничества является использование чат-ботов. Чат-бот (англ. chatbot) – программа, которая имитирует реальный разговор с пользователем. Чат-боты позволяют общаться с помощью текстовых или аудиосообщений на сайтах, в мессенджерах, мобильных приложениях или по телефону. Согласно информации на

официальном интернет-сайте Национальной полиции Украины, правонарушители, воспользовавшись ситуацией в стране из-за пандемии Covid-19 и карантином в государстве, размещают в интернете видеозапись, в которой Президент Украины говорит о материальной помощи и выплате денежной компенсации для предпринимателей. В описании к видеозаписи мошенники дают ссылку на ресурс, на котором якобы можно подать заявку на получение выплаты, убеждая, что данные компенсации может получить каждый. При использовании указанной ссылки человек переходит в чат-бот, который визуально не отличается от официального чат-бота «Ощадбанка», и ему предлагается ввести персональные данные и номер банковской карты для зачисления денег. Затем мошенники просят оплатить услуги по оформлению заявления, получению электронной подписи, прохождению идентификации и т. п. Доверчивые граждане, желая получить денежную компенсацию, выполняют перечисление денег и после этого их доступ к чат-боту блокируется.

Учитывая вышеизложенное, можно сделать вывод о том, что на сегодняшний день мошенничество с помощью мобильного телефона основывается на использовании современной электронно-вычислительной техники.

Одним из действенных способов борьбы с данным видом мошенничества, на наш взгляд, может стать введенный в Украине на законодательном уровне контроль приобретения и использования сим-карт путем регистрации их в электронной базе с привязкой к паспортным данным покупателя, а также предоставление упрощенного доступа к этой базе данных сотрудникам, осуществляющим расследования преступлений, связанных с использованием мобильной связи.

УДК 343.8

Д.Б. Данилов

О ЗАКОНОДАТЕЛЬНОМ ЗАКРЕПЛЕНИИ ПОНЯТИЯ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ «ПОЛУЧЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

С развитием информационных технологий трансформируются способы совершения преступлений и обмена информацией согласно новейшим тенденциям в обществе. Наряду с изменениями в криминальной среде, происходит совершенствование механизма работы правоохранительных органов по выявлению, предупреждению, пресечению и раскрытию преступлений. В последнее время использование электронных устройств

обработки и хранения информации стало неотъемлемой частью жизни современного общества. При этом их используют в своей деятельности как криминальный элемент, так и правоохранительные органы, в частности сотрудники оперативных подразделений органов внутренних дел при осуществлении оперативно-розыскной деятельности.

Для того чтобы полностью применять все многообразные инструменты поиска оперативно-значимой информации, необходимо непрерывно совершенствовать нормативно-правовую базу в области оперативно-розыскной деятельности.

В настоящее время в России происходит информатизация общества, и большая часть данных, передаваемых и воспринимаемых человеком, преобразуется в информацию, обрабатываемую и передаваемую с помощью компьютерных устройств. Из-за необходимости разъяснения понятия компьютерной информации изменяется и дополняется законодательная база, которая непрерывно совершенствуется и является довольно динамичной. Так, Федеральным законом от 6 июля 2016 г. № 374-ФЗ в Федеральный закон «Об оперативно-розыскной деятельности» введено новое оперативно-розыскное мероприятие – «получение компьютерной информации». Введение данного оперативно-розыскного мероприятия обусловлено активным использованием сети Интернет криминальными структурами и элементами в целях координации своих действий и получения информации, необходимой для осуществления преступной деятельности.

Члены научного сообщества России высказывали различные мнения о целесообразности внесения в нормативно-правовую базу, регулирующую оперативно-розыскную деятельность, разъяснений в отношении нового вида оперативно-розыскного мероприятия – «получение компьютерной информации». Однако до сих пор законодатель не определил организационно-тактический порядок его проведения и не дал исчерпывающих пояснений самого понятия «получение компьютерной информации». Законодатель в ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» дает общее понятие информации: информация – сведения (сообщения, данные) независимо от формы их представления. Чтобы уточнить, что является компьютерной информацией, следует обратиться к УК РФ. Лишь в прим. 1 к ст. 272 УК РФ дано пояснение данного понятия: под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

В соответствии с Соглашением о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации, ратифицированном Федеральным