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

законом от 1 октября 2008 г. №164-ФЗ под компьютерной информацией понимается информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи.

А.Ф. Мицкевичем, А.В. Суслопаровым на основе отечественного и зарубежного опыта было проведено исследование понятия компьютерная информация. Они пришли к выводу, что под компьютерной информацией следует понимать сведения, передающиеся между субъектами посредством сигналов в форме электронного кода, пригодного для обработки сведений компьютерными средствами. Наличие кода, как и остальных характерных особенностей компьютерной информации, предполагает нахождение данных в компьютерной системе.

Под указанную трактовку компьютерной информации попадает, скорее, не конкретная информация, а ее форма представления, а именно доступная для восприятия электронно-вычислительной машиной (ЭВМ). В качестве ЭВМ может выступать технические устройства, начиная с персонального компьютера, сервера и иного промышленно-вычислительного оборудования и заканчивая смартфоном.

Содержание оперативно-розыскного мероприятия «получение компьютерной информации» выражается в способах реализации задач по поиску, регистрации и фиксации информации, которая представлена в конечном итоге в виде двоичного кода и не может восприниматься без использования специализированных устройств ввода-вывода данных непосредственно человеком.

Способы доступа к компьютерной информации в зависимости от формы контакта с ней можно разделить: на непосредственные; опосредованные, или удаленные; комплексные, или смешанные.

Одним из способов получения компьютерной информации является негласное получение дистанционного, или удаленного, доступа к устройствам, предназначенным для автоматизированной обработки оцифрованных данных (сетевые и персональные компьютеры, планшеты, смартфоны и др.) лицом, представляющим оперативный интерес, путем преодоления защиты доступа специальными техническими устройствами либо программами. Данный способ возможно использовать, лишь имея специальные технические познания либо привлекая специалистов.

Иной способ получения доступа к данным, находящимся на устройствах, предназначенных для автоматизированной обработки оцифрованных данных, – негласное получение непосредственного доступа к устройствам и носителям информации с последующими копированием или анализом данных, осуществляемым непосредственно с устройства.

Таким образом, получение компьютерной информации – поиск и получение доступа к сведениям (данным), хранящимся на электронных носителях информации и обрабатываемым устройствами обработки данных, путем использования устройств ввода-вывода и хранения данных с целью последующего приема, передачи, записи, регистрации, хранения либо непосредственного восприятия человеком.

Считаем целесообразным включение предлагаемой нами дефиниции в ведомственный нормативный правовой акт МВД России, а также последующую разработку организации и тактики проведения оперативно-розыскного мероприятия «получение компьютерной информации».

УДК 343.985

А.А. Дедковский

ОПЕРАТИВНО-РОЗЫСКНОЕ ОБЕСПЕЧЕНИЕ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ

Анализ правоприменительной практики Республики Беларусь свидетельствует о том, что состояние преступности характеризуется не ростом киберпреступлений, а фактическим стиранием границ, разделявших их с иными традиционными для нашего общества преступлениями. Появление в Республике Беларусь новых способов совершения криминальных деяний с использованием криптовалют в настоящее время характерно не только для преступлений против собственности (ст. 209, 212 УК) и информационной безопасности (несанкционированный доступ к компьютерной информации (ст. 349 УК), компьютерный саботаж (ст. 351 УК), неправомерное завладение компьютерной информацией (ст. 352 УК), использование вредоносных программ (ст. 354 УК)), но и для таких связанных с легализацией (отмыванием) средств, полученных преступным путем, преступлений, как незаконный оборот наркотических средств (ст. 328 УК), изготовление и распространение порнографических материалов, в том числе с изображением несовершеннолетнего (ст. 343, 343^1 УК), организация незаконной миграции (ст. 371^1 УК), вымогательство (ст. 208 УК) и др. Несмотря на высокую латентность таких преступлений и отсутствие целенаправленного учета, в 2020 г. возбуждено более 100 уголовных дел, в которых фигурирует криптовалюта, если не как предмет преступного посягательства, то как средство достижения преступного результата.

Качественным отличием деяний, механизм которых предусматривает использование IT-технологий, от традиционных преступных посяга-