По нашему мнению, определение ОРМ, которое содержится в Законе «Об оперативно-розыскной деятельности», не отражает существенных признаков, которыми они должны обладать. Полагаем, что под ОРМ следует понимать санкционированные прокурором (судьей) и охраняемые уголовным законом негласные действия, организация и тактика которых образуют сведения, составляющие государственные секреты, проводимые уполномоченными должностными лицами органов, осуществляющих ОРД, в отношении физических лиц при наличии установленных в законодательстве оснований и условий, направленные на познание объективной действительности, имеющей значение для решения задач ОРД, с возможностью применения специальных технических средств, ограничения прав и свобод личности, а также привлечения к подготовке или участию в них третьих лиц. Принятие законодателем авторского подхода к определению ОРМ повлечет за собой изменение количества, наименования ОРМ, а также оснований для их проведения. Многие из ныне существующих ОРМ, такие как «оперативный опрос», «наведение справок» с целью получения сведений, не составляющих охраняемую законом тайну, «наблюдение» в общественном месте, «оперативный осмотр», проводимый вне жилища, и некоторые другие, не отвечают авторскому определению ОРМ, поэтому их, по нашему мнению, необходимо исключить из перечня ОРМ.

Исходя из нового понимания ОРМ, под основаниями для их проведения следует рассматривать ставшие известными органам, осуществляющим ОРД, сведения: о событиях и действиях, создающих угрозу национальной безопасности Республики Беларусь; наличии признака преступления; лице, могущем располагать информацией, необходимой для решения задач ОРД; исчезновении лица.

УДК 343.985

А.М. Шинкевич, Н.Г. Букшта

ПРЕСТУПНОСТЬ В СЕТИ ИНТЕРНЕТ

Ежегодно наблюдается рост преступлений в сети Интернет, при этом оперативные сотрудники отмечают, что средства и способы совершения данных преступлений постоянно видоизменяются. Совершая преступления злоумышленники убеждены, что через сеть Интернет гораздо проще и быстрее обмануть жертву, чем в процессе личного общения, а благодаря использованию специально приспособленного программного обеспечения правоохранительные органы не в состоянии их выявить.

Условно можно выделить две основные преступные схемы, используемые злоумышленниками в сети Интернет. Первая схема предполагает введение в заблуждение неограниченного количества лиц, часть из которых в конечном итоге станет жертвой преступления, вторая направлена на обман конкретных лиц, сведения о которых заранее известны злоумышленникам. Обе схемы сопряжены с завладением имущества жертвы посредством отчуждения этого имущества самой жертвой или противоправного получения доступа к возможности распоряжаться этим имуществом.

При реализации первой схемы злоумышленники посредством сети Интернет на сайтах, форумах, мессенджерах под видом взломанных платных программ размещают вредоносные файлы. Потенциальные жертвы скачивают и устанавливают на свои мобильные устройства (смартфон, планшет, ноутбук и т. д.) якобы взломанные платные программы, при этом вредоносные файлы, скрытно от пользователя устанавливаются на мобильное устройство, после чего собирают и передают преступникам через сеть Интернет конфиденциальную информацию, хранящуюся на мобильном устройстве жертвы. Заполучив информацию, у злоумышленников появляется возможность распоряжаться имуществом жертвы.

Кроме вредоносных программ злоумышленники также размещают провокационную информацию о возможности пользователям сети Интернет получить материальную выгоду (всевозможные платные опросы, конкурсы, лотереи и т. д.). Прочитав эту информацию, в надежде на обогащение пользователи сети Интернет действуют по заранее предписанному им алгоритму, который, как правило, автоматизирован. Не осознавая возможных последствий, они скачивают и запускают замаскированные вредоносные файлы, на фишинговых интернет-страницах вводят свои персональные данные, данные банковских платежных карт, электронных кошельков, номера телефонов, пришедших им на телефон СМС-кодов, логинов и паролей, полагая, что они находятся на официальной странице сайта, предоставляющего им услуги, либо самостоятельно осуществляют оплату по предоставленным злоумышленниками реквизитам.

Провокационная информация может размещаться в группах, каналах, сообществах защищенных мессенджеров, социальных сетях с возможностью обратной связи. Изучив информацию, потенциальные жертвы самостоятельно начинают устанавливать связь с злоумышленниками. Последние, в свою очередь, используя методы социальной инженерии, в ходе общения (переписки) с обратившимися создают иллюзию возможности обогатиться, убеждают в реальности размещенной информации,

вынуждая жертву действовать по заранее разработанному плану, предполагающему получение конфиденциальной информации либо оплату за оказываемые фиктивные услуги. Как правило, жертвами преступников становятся неопытные доверчивые пользователи, которые уверены, что через сеть Интернет можно заработать, при этом необязательно иметь какие-то специальные знания в области информационных технологий, достаточно выполнить некий алгоритм (в основном это дети, пожилые люди или просто наивные лица). Жертвами движет желание обогатиться за короткий промежуток времени с минимальными затратами. Такое желание присуще многим людям, поэтому преступность в сети Интернет широко распространена.

В мессенджере Telegram в различных группах и на каналах активно размещаются объявления о продаже различных схем заработка («белых», «серых», «черных»). При этом схемы заработка могут быть нерабочими, нереальными или вовсе отсутствовать и, как правило, при этом осуществляется предоплата.

В процессе реализации второй преступной схемы злоумышленники заранее целенаправленно изучают жертву (например, через социальные сети, банки и базы данных, форумы, группы, знакомых и иным способом) с целью определения наиболее подходящего способа введения в заблуждение и возможности преступного обогащения. Продумывается способ получения имущества или информации, необходимой для доступа к распоряжению этим имуществом (например, доступ к интернет-банкингу, электронному кошельку, аккаунту и т. д.). Можно выделить несколько таких способов. Первый способ предполагает получение этого имущества в процессе непосредственного удаленного общения с самой жертвой, которая соглашается помочь злоумышленнику, при этом последний часто выдает себя за знакомого, друга, родственника, например общение через социальные сети со страницы знакомого с просьбой одолжить денег или оплатить товар, работу или услугу. Второй способ сводится к скрытой удаленной или непосредственной установке на мобильное устройство жертвы специального вредоносного программного обеспечения, способного собирать и передавать через сеть Интернет конфиденциальную информацию, хранящуюся на мобильном устройстве, с использованием которой злоумышленники распоряжаются имуществом жертвы.

В настоящее время оперативные сотрудники органов внутренних дел вследствие различных причин наравне с выявлением преступлений в сети Интернет в большей степени занимаются проверкой информации по заявлениям обратившихся жертв этих преступлений. Предпосылок, способствующих этому, много. В первую очередь, это цифровая трансформация сферы товаров, работ и услуг (переход на безналичные платежи), возможность создания и распространения вредоносного программного обеспечения, которое используют злоумышленники, отсутствие запрета на использование программного обеспечения, подменяющего место выхода в сеть Интернет, использование зарубежных мессенджеров, основанных на технологии шифрования данных, распространение среди населения в качестве средства платежа криптовалюты. Для качественного выявления преступлений в сети Интернет сотрудники должны проходить обучение за рубежом в развитых государствах с цифровой экономикой, где накоплен богатый опыт обучения и противодействия преступности в сети Интернет, используются передовые цифровые технологии по автоматизации анализа информации в сети Интернет, банков и баз данных.

УДК 343.985

И.И. Шишковец

ОБ ИСПОЛЬЗОВАНИИ МАТЕРИАЛОВ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ДЛЯ ФОРМИРОВАНИЯ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ ПРОЦЕССЕ

Оперативно-розыскная деятельность направлена на решение разноплановых задач, связанных с получением сведений о событиях и действиях, создающих угрозу национальной безопасности Республики Беларусь, с предупреждением, выявлением, пресечением преступлений, выявлением лиц, их подготавливающих, совершающих или совершивших, розыском скрывшихся лиц и т. д. ОРД является самостоятельным видом деятельности оперативных подразделений соответствующих государственных органов Республики Беларусь, выступающим адекватным инструментом борьбы с тайными (скрытыми) преступными проявлениями и требующим эффективного правового регулирования всего ее процесса и результата. Эта деятельность находит отражение в соответствующих материалах, к которым относятся оперативно-служебные документы (постановление о проведении ОРМ, специальное задание, протокол ОРМ, справка, рапорт, акт, письменный запрос органа, осуществляющего ОРД, и иные документы, образующиеся при ее осуществлении) и материальные носители информации, содержащие сведения о проведении ОРМ, а также иные сведения и документы, полученные при осуществлении ОРД.