Второе направление предусматривает первоочередный допрос свидетелей из числа «приближенных» подозреваемому лиц (подчиненные, лица, в чьих интересах совершено злоупотребление, и т. д.). Данное положение оптимально применять в ситуациях, обусловленных внезапностью возбуждения уголовного дела для подозреваемого либо ситуацией его минимальной информированности о ходе и результатах расследования, когда он не успевает договориться со свидетелями. Использование фактора внезапности на первоочередном допросе информированных о противоправной деятельности подчиненных и руководителей подозреваемого может улучшить благоприятность ситуации, так как указанная группа свидетелей будет беспокоиться за свою персональную ответственность и последствия противоправной деятельности. Кроме того, в рассматриваемой ситуации оптимальным будет проведение одновременного допроса указанных групп в рамках следственной группы.

С учетом вышеизложенного представляется возможным сформулировать следующие выводы:

особенности допроса свидетелей по делам о злоупотреблении властью или служебными полномочиями заключается в тематике допроса, содержании сведений, получаемых от допрашиваемых лиц, в последовательности вызова на допрос различных категорий свидетелей, а также в тактических приемах их допроса;

круг лиц – потенциальных свидетелей по указанной категории дел – можно разделить на следующие категории: руководители подозреваемого (обвиняемого) разного звена; сотрудники, подчиненные подозреваемому (обвиняемому) по службе; сослуживцы подозреваемого (обвиняемого); близкие подозреваемому (обвиняемому) лица; лица, в чьих интересах совершено преступление; иные лица, которые располагают сведениями, значимыми для расследования дела;

выбор наиболее целесообразных тактических приемов допроса и типовой перечень вопросов, подлежащих выяснению у свидетелей по делам о злоупотреблении властью или служебными полномочиями, зависит от отнесения свидетеля к той либо иной группе и мотивов, влияющих на позицию свидетеля относительно достоверности и полноты дачи им показаний.

Список использованных источников

1. Ульянов, Д. В. Расследование злоупотребления должностными полномочиями : дис. … канд. юрид. наук : 12.00.09 / Д. В. Ульянов. – Люберцы, 2011. – 228 л.

2. Халиков, А. Н. Следственные действия по делам о должностных преступлениях: система, характеристика, тактика / А. Н. Халиков. – М. : Юрлитинформ, 2008. – 235 с.

3. Зорин, Г. А. Руководство по тактике допроса : учеб.-практ. пособие / Г. А. Зорин. – М. : Юрлитинформ, 2001. – 320 с.

4. Печерский, В. В. Типовые программы допроса : пособие / В. В. Печерский. – Гродно : ГрГУ, 2002. – 160 с.

Дата поступления в редакцию: 18.10.2023

УДК 343.985.8

***Б. В. Ковалик**, адъюнкт научно-педагогического факультета*
Академии Министерства внутренних дел Республики Беларусь
e-mail: boriskovalik@yandex.ru

О МЕХАНИЗМЕ СОВЕРШЕНИЯ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ ДИСТАНЦИОННЫМ СПОСОБОМ

Проанализированы научные взгляды на проблему формирования информационной модели преступления в оперативно-розыскной деятельности. Обоснована целесообразность ее формирования через механизм совершения преступления. С применением данного подхода сформирован механизм совершения дистанционных мошенничеств без привязки к конкретным способам его совершения. Выделены три этапа совершения преступлений данного вида и дана характеристика каждого из них. Описаны особенности каждого из этапов.

Ключевые слова: оперативно-розыскная деятельность, механизм совершения преступления, мошенничество в сети Интернет.

***B. V. Kovalik**, Postgraduate Student of the Scientific and Pedagogical Faculty of the Academy of the Ministry of Internal Affairs of the Republic of Belarus, e-mail: boriskovalik@yandex.ru*

ON THE MECHANISM OF COMMITTING REMOTE FRAUD BY REMOTE MEANS

The article presents the analysis of scientific views on the problem of formation of the information model of crime in detective activity. The expediency of its formation through the mechanism of committing a crime is substantiated. With the use of this approach the mechanism of committing remote frauds without reference to specific ways of its commission is formed. Three stages of committing crimes of this type are distinguished and each of them is characterized. The peculiarities of each of the stages are described.

Keywords: detective activity, mechanism of committing a crime, Internet fraud

Механизм совершения большинства преступлений чаще всего состоит из трех этапов: начального, основного, завершающего, которые являются звеньями одной цепи, объединенными единым целеполаганием. В то же время каждый из этапов может рассматриваться в качестве целостного, относительно самостоятельного процесса, автономного вида целенаправленной человеческой деятельности, сочетающей в себе организационные, познавательные и конструктивные моменты [1, с. 21]. Механизм совершения мошенничеств дистанционным способом отличается своей сложностью, что более обусловлено транснациональным составом преступных групп, которые преимущественно осуществляют данную противоправную деятельность на территории Республики Беларусь. Немаловажным фактором, осложняющим установление лиц, вовлеченных в данный вид противоправной деятельности, на наш взгляд, является то, что в большинстве случаев у преступников нет необходимости лично контактировать с потерпевшим или другими членами преступной группы.

В контексте деталей рассматриваемого вида преступления существенно отметить, что меры для дальнейшего сокрытия следов преступления и сохранения собственной анонимности мошенники предпринимают на всех трех этапах совершения преступления, что характерно и для других преступлений, совершаемых с использованием компьютерной техники [2, с. 152].

По сути, при смене легенды и даже способа совершения мошенничества как таковой его механизм не претерпевает кардинальных изменений и только адаптируется под избранную злоумышленником обстановку, конкретную жертву и т. д. Анализ наиболее распространенных на территории Республики Беларусь схем мошенничеств, совершенных дистанционным способом, дает возможность составить общее представление о механизме их совершения.

Концепция формирования оперативно-розыскной характеристики преступления (далее – ОРХП) с учетом механизма его совершения недостаточно распространена среди исследователей оперативно-розыскной деятельности (ОРД). Общепринятым инструментом изучения преступного деяния в контексте ОРД считается ОРХП, составленная с применением элементного подхода. Однако, на наш взгляд, разработка типовой модели механизма совершения мошенничества дистанционным способом не вызывает противоречий и отражает особенности данного преступления, что повышает продуктивность и результативность деятельности правоохранительных органов по борьбе с мошенническими проявлениями. В данной связи обоснованно согласиться с мнением Д. В. Ермоловича в том, что понимание механизма мошенничества и его отдельных составляющих несет в себе ценность для дальнейшей разработки рекомендаций по «оперативному сопровождению» уголовных дел о мошенничестве [3, с. 110].

Разработка типовой модели совершения мошенничества дистанционным способом с учетом механизма его совершения в том числе обусловлена быстрой сменой мошеннических схем, реализуемых на территории Республики Беларусь. В связи с этим рассмотрение мошенничеств, совершаемых дистанционно, не привязываясь к конкретным способам его совершения, видится логичным, так как при попытках разработки классификаций по данному признаку большинство авторов сталкиваются с проблемой, обозначенной еще И. Н. Якимовым. По его мнению, способы мошенничества совершенно не поддаются какой-либо научной классификации, потому что обман так же разнообразен, как человеческая изобретательность [4, с. 401]. Определенная значимость данного подхода для ОРД заключается и в том, что подробное описание каждого из этапов

исследуемого преступления позволяет эффективнее устанавливать причастных к его совершению лиц еще на стадии подготовки к его совершению.

Описывая начальный (подготовительный) этап, следует отметить, что выработать исчерпывающий перечень подготовительных действий преступника, совершающего мошенничество дистанционным способом, видится затруднительным. В этой связи логично перечислить наиболее часто встречающиеся из них.

На данной стадии совершения преступления мошенники, как правило, предпринимают следующие действия: выбирают легенды мошенничества; определяют обстановку совершения мошеннических действий; подбирают орудия и средства совершения преступления; определяют количество необходимых соучастников и подбирают соответствующих исполнителей; осуществляют поиск жертвы.

Под легендой мошенничества стоит понимать сведения, предоставляемые преступником потенциальной жертве с целью убеждения последнего в том, что злоумышленник действительно является тем, за кого себя выдает (сотрудник банка или правоохранительных органов; родственник, попавший в беду; продавец или покупатель товара и услуги и др.). Ряд авторов соотносят понятие легенды мошенничества со способом его совершения [5, с. 6]. Однако, на наш взгляд, способ совершения мошенничества – более широкое понятие. Легенда мошенничества, по сути, является только предлогом для коммуникации с потенциальной жертвой, что напрямую не влечет за собой реализацию преступных намерений мошенника. Чаще всего дальнейший алгоритм действий мошенника кардинально не меняется в зависимости от выбора той или иной легенды мошенничества.

Легенда мошенничества тесно связана с выбором злоумышленниками обстановки для совершения преступления, в качестве которой, как правило, выступает тот или иной ресурс глобальной сети Интернет: классифайды[1], социальные сети, профильные сайты знакомств, мессенджеры и т. п. Составление легенды мошенничества зависит от конкретного функционала и направленности того или иного интернет-ресурса, в связи с чем обычно обстановка в данной цепи является первичной. Но возможен вариант, когда уже отработанная ранее легенда может быть адаптирована под смежный, не являющийся профильным в той или иной сфере, ресурс.

После выбора ресурса мошенники совершают ряд подготовительных действий по подбору и подготовке орудий и средств совершения преступления. Данные действия могут выражаться в целом комплексе действий: приобретении необходимых средств компьютерной техники; регистрации аккаунтов на различных ресурсах; приобретении виртуальных SIM-карт; установке или разработке дополнительного программного обеспечения (ПО); регистрации доменов для генерации фишинговых ссылок на существующие сайты либо создание новых подложных сайтов, если этого требует легенда мошенничества; регистрации виртуальных банковских платежных карт (БПК), электронных либо криптовалютных кошельков для вывода похищенных средств и др. Конкретный перечень орудий и средств определяется злоумышленниками уже после выбора легенды мошенничества и обстановки ее реализации и может корректироваться в зависимости от складывающихся обстоятельств в процессе осуществления преступного замысла. Необходимо отметить, что один и тот же предмет в различных условиях может выступать как в качестве орудия, так и в качестве средства совершения преступления.

В зависимости от конкретного сценария совершаемого мошенничества может различаться количество соучастников. Кроме того, на численность соучастников в каждом конкретном случае может влиять факт вовлечения злоумышленника в преступную группу. Большинство преступных схем, используемых мошенниками сегодня, гипотетически можно реализовать в одиночку, что связано с отсутствием необходимости непосредственно контактировать с потенциальной жертвой. Таким образом, один человек может одновременно выдавать себя и за покупателя, который уверяет, что перевел пострадавшему денежные средства за товар, и за мнимого оператора службы поддержки, который в онлайн-чате фишингового ресурса уверяет его в том, что транзакция проведена, но зачисление денежных средств задерживается по техническим причинам. Однако в одиночку мошенники обычно действуют только при реализации самых примитивных

[1] Классифайд – онлайн-сервис, на котором аккумулируются различные сгруппированные по темам объявления от частных лиц и компаний.

схем, не дающих возможности получения крупного преступного дохода, а также несущих в себе большие риски деанонимизации и дальнейшего привлечения к ответственности.

На данный момент большинство мошеннических схем на территории Республики Беларусь реализуется преступными группами. Таким образом, непосредственный исполнитель получает доступ к подробным инструкциям по реализации того или иного сценария и не обременен решением вопросов организационного и технического обеспечения преступной деятельности. За подобное сотрудничество рядовой мошенник, именуемый на сленге «воркером», отдает часть приобретенных преступным путем денежных средств и взамен получает устные гарантии организаторов об обучении, высоком проценте и скорости выплат по сделкам, всесторонней технической поддержке и исключения факта привлечения к ответственности при соблюдении всех рекомендаций кураторов [6, с. 101].

Для реализации преступных схем, согласно которым потенциальная жертва должна передать наличные денежные средства, дополнительно задействуется курьер. Являясь наиболее уязвимым участником преступной схемы, последний непосредственно контактирует с жертвой преступления и не имеет фактической возможности осуществлять собственную деятельность за пределами Республики Беларусь в отличие от остальных злоумышленников. Высокая вероятность задержания курьеров очевидна и для администрации преступных групп. По данной причине их осведомленность ограничивается никнеймом вербовщика или куратора в мессенджере для минимизации утечки сведений о преступной группе в случае сотрудничества курьера с правоохранительными органами.

Вербовка непосредственных исполнителей в большинстве случаев осуществляется через специально предназначенные телеграмм-боты, ссылки на которые можно найти на тематических форумах, как правило, в теневом сегменте сети Интернет. Подбор курьеров может осуществляться путем размещения объявлений с предложениями о высокооплачиваемой подработке на ресурсах, не имеющих отношения к преступной деятельности, или путем рассылки через мессенджеры. Их текст содержит сведения о легальных вакансиях курьеров. В дальнейшем лицо, выразившее желание работать, перенаправляется в телеграмм-бот или проходит собеседование с куратором. В ходе беседы куратор может потребовать предоставить фото паспорта, ответить на видеозвонок и т. д. Данные сведения в последующем могут использоваться для шантажа мошенника в случае возникновения внештатных ситуаций для куратора. Кандидата осведомляют о криминальном характере деятельности и процентном соотношении вознаграждения за работу.

Отдельно вполне обоснованно стоит отметить лиц, непосредственно не вовлеченных в преступный процесс, но случайно втянутых в данное событие и не предполагающих, что они являются его косвенными соучастниками. Некоторые из них, например, посредники, именуемые «дропами», сознательно соглашающиеся стать трансфером денег, собираемых мошенниками, либо предоставить другие услуги, используя свои персональные данные, чаще всего предполагают, что вовлечены в какой-либо преступный процесс. Но наряду с ними имеют место случаи неосознанного способствования осуществлению мошеннических действий со стороны законопослушных субъектов. Такими могут явиться добросовестные обменщики криптовалюты; организации, предоставляющие рекламные услуги в сети Интернет, в том числе на поисковых сервисах и т. д. Сами потенциальные жертвы до осознания факта совершения в отношении них противоправных действий могут порекомендовать подложный сервис своим знакомым либо продолжить цепь рассылки сведений о фальшивых розыгрышах и т. п., тем самым оказать содействие мошенникам по вовлечению новых жертв. Следовательно, лица, случайно втянутые в преступное событие, могут оказывать помощь злоумышленникам на всех этапах его совершения.

На начальном этапе формирования механизма преступления значимую роль играет выбор потенциальной жертвы. От ее виктимности, т. е. образа действий или бездействия, при которых она становится жертвой преступления, в значительной мере зависит, реализует ли преступник свои намерения. Жертва любого мошенничества обычно проявляет неосмотрительность, что увеличивает ее подверженность умышленным преступным посягательствам. В большинстве случаев совершение данного вида преступления становится возможным только потому, что пострадавшие в период поиска преступником жертвы, по труднообъяснимым причинам доверяются случайным людям. Часто это бывает вызвано некомпетентностью жертвы в том или ином вопросе.

Как правило, мошенники, совершая описываемый вид хищения дистанционным способом, ищут новых потенциальных жертв, опираясь на данный критерий. Наличие большого количества пострадавших от описываемого вида преступления в Республике Беларусь, на наш взгляд, в том числе объясняется низким уровнем банковской и цифровой грамотности населения. По указанной причине жертвами преступников чаще становятся пожилые люди, которые в разы сложнее воспринимают внедрение современных технологий в различные сферы жизнедеятельности.

Поиск потенциальной жертвы может осуществляться «активным» и «пассивным» способом. Примером первого может служить обращение мошенника к конкретному лицу по конкретному вопросу: о покупке товара, о продаже которого гражданин разместил объявление; знакомство в социальной сети или на профильном сервисе с перспективой дальнейшей встречи интимного характера и т. п. «Пассивный» поиск может осуществляться путем массовой рассылки либо запуска рекламы на специализированных интернет-сервисах. Предлогом может служить проведение рекламной игры с большим призовым фондом, распродажа товара по выгодной цене, реклама быстрых способов заработка, сбор денежных средств в благотворительных целях, просьба о помощи и т. д.

Если в первом случае мошенник самостоятельно пытается вычленить из массы пользователей гражданина, склонного к беспечным необдуманным действиям, то во втором – потенциальная жертва отзывается на предложение преступников самостоятельно, не обращая внимания на косвенные признаки предстоящего преступления.

Стоит также отметить и то, что осуществление подготовительных действий к совершению мошенничества дистанционным способом, может выражаться как в реализации некриминальных действий, так и быть сопряженным с совершением уголовно наказуемых деяний. Примером последних могут служить: хищение устройств, с которых осуществлена авторизация в учетные записи владельца; осуществление несанкционированного доступа к компьютерной информации, чаще всего выраженном во взломе аккаунтов в социальных сетях, и др.

Осуществив подготовительные действия, злоумышленник переходит к основному рабочему этапу. На данном этапе мошенники вовлекают жертву в легенду мошенничества и в последующем склоняют ее к непосредственной передаче денежных средств.

Формирование у потерпевшего намерений совершить действия, предлагаемые мошенником, осуществляется, как правило, путем вызова у человека сильных эмоций, связанных скорее с возможностью получения выгоды, либо напротив, избежания наступления серьезных негативных последствий. Таким образом, злоумышленник склоняет жертву к принятию якобы выгодного или единственно возможного для него решения.

Для достижения цели мошенники используют методы социальной инженерии, являющейся собирательным термином для обозначения социопсихологических манипуляций, используемых злоумышленниками для получения доступа к защищенным системам с целью кражи информации, паролей, данных о БПК, склонения к определенным действиям и т. п. [7, с. 19]. По мнению А. Л. Осипенко, для злоумышленников социальная инженерия работает намного продуктивнее, чем применение «прямого взлома» [2, с. 153].

В дальнейшем злоумышленник просит жертву выполнить определенные условия: внести предоплату за покупку/доставку товара; привязать карту к определенному сервису для вывода полученной прибыли; заказать такси либо выбрать подарок для девушки, которая готова к встрече; передать денежные средства определенному лицу, установить стороннее программное обеспечение на личный мобильный телефон или персональный компьютер и т. п.

Когда потенциальная жертва принимает условия, предложенные мошенником, последний принимает меры по непосредственному завладению денежными средствами. В зависимости от ранее определенных обстоятельств это может происходить как путем онлайн-перевода, так и посредством передачи наличных денежных средств курьеру.

Так, в случае передачи денежных средств курьеру действия развиваются следующим образом: курьер уточняет адрес у куратора, выбывает к жертве и непосредственно завладевает денежными средствами. Все время, вплоть до получения от курьера сведений о передаче денежных средств, потерпевший остается на связи с преступниками. Несмотря на простоту реализации, данный способ трансфера денежных средств требует дополнительных мер на завершающем этапе и несет в себе дополнительные риски для злоумышленников.

В случае завладения денежными средствами путем онлайн-платежа, мошенник просит потенциальную жертву перейти по предоставленной им ссылке и выполнить условия рекомендуемого сервиса, который является фишинговым. Чаще всего мошенники не сталкиваются с проблемами генерации фишинговых ссылок. Ранее в каждом конкретном случае исполнитель запрашивал ссылку у куратора. Сейчас им, как правило, предоставлен доступ к телеграмм-ботам, автоматизировавшим данный процесс. Для ее получения необходимо отправить в бот ссылку на нужный товар и т. п., после чего скрипт[1] самостоятельно создает подложную страницу в зависимости от заданной конфигурации.

Страница, отображаемая после перехода по ссылке, является оболочкой для сбора данных о карте потерпевшего – маской платежной системы для P2P перевода[2]. После ввода данных БПК в предоставленную форму, их получают мошенники и вносят в заранее подготовленное поле для перевода денег. Банк реагирует на запрос и отправляет код 3D-secure[3]. Жертва считает, что код пришел для подтверждения операции, осуществляемой в окне мнимого сервиса, так как все действия осуществляются параллельно с минимальной временной задержкой. После ввода кода в подготовленное на фишинговой странице поле он попадает к мошенникам. Таким образом, злоумышленники получают возможность подтвердить списание средств с карты пострадавшего.

Отмеченные алгоритмы, как правило, применяются организованными группами. Мошенники, не вовлеченные в преступные формирования, чаще всего предоставляют потенциальной жертве реквизиты своей или ассоциированной с ними БПК, благодаря которым их дальнейшая идентификация не вызывает трудностей.

На протяжении общения с потерпевшим мошенник анализирует его поведение и на основании полученных сведений делает вывод о возможности повторной попытки совершения преступного посягательства на денежные средства жертвы. После первого списания денежных средств злоумышленники пытаются выяснить, остались ли на счету потерпевшего денежные средства. Это может быть реализовано путем предоставления ссылки на якобы возврат средств по причине сбоя в работе банка и т. п. Там потерпевшему снова необходимо ввести данные БПК, однако это сделано только для минимизации подозрений, так как данные карты у мошенников уже есть. Фактически мошенникам необходимо узнать новый код 3D-secure для повторного списания. Часто преступники узнают сведения об оставшемся балансе у самого потерпевшего. В подобных ситуациях его просят прислать скриншот SMS-оповещения от банка для подтверждения факта оплаты, где кроме суммы списания, отображается остаток на счете. Мошенник также может ввести потерпевшего в заблуждение, сообщив о невозможности платежа по причине того, что на балансе БПК должно находиться не менее определенной суммы денежных средств. Часто в ответ на это потерпевший сам сообщает текущий баланс, пытаясь доказать мнимому оператору, что причина в другом. Существует иной способ выяснения точного баланса БПК, когда окно для введения данных сведений встроено в подложный платежный сервис, однако такой подход обычно вызывает подозрения у потенциальных жертв и используется все реже.

Онлайн-перевод также может быть осуществлен без непосредственного участия жертвы. Для этого мошенники склоняют пострадавшего к установке на находящееся в его пользовании средство компьютерной техники ПО для осуществления к нему удаленного доступа. Как правило, злоумышленники обосновывают необходимость установки подобных приложений, выдавая их за ПО, разработанное службой поддержки той или иной банковской организации. Таким образом, злоумышленники получают возможность воспользоваться сохраненными на устройстве паролями, прочитать SMS-сообщение с отправленным банком кодом 3D-secure и т. п.

Подобные ситуации служат примером адаптации мошенниками различных средств для реализации преступного замысла. Подобное ПО легально размещается в онлайн-магазинах приложений для операционных систем Android и iOS и по своему целевому назначению не является вредоносным, но используется злоумышленниками в противоправных целях.

---

[1] Скрипт (от англ. script – сценарий) – простейшая компьютерная программа, содержащая последовательность действий, созданная для автоматического выполнения определенных задач.

[2] P2P перевод – технология онлайн-перевода средств с карты на карту одноранговыми пользователями.

[3] 3-D Secure – протокол, используемый как дополнительный уровень безопасности онлайн-кредитных и дебетовых карт, для двухфакторной аутентификации пользователя.

Важно указать, что произошедшие на данном этапе изменения в образе действий потерпевшего, например, отказ выполнения или неверная интерпретация требований мошенника, могут служить препятствием к достижению их преступного замысла, вплоть до невозможности его осуществления или нести в себе риск задержания курьера, если последний задействован в избранной преступниками схеме.

По мнению А.М. Кустова, формирование завершающего этапа механизма преступления в большинстве случаев характеризуется наступлением преступного результата замышляемого деяния [1, с. 26]. Применительно к мошенничествам, совершаемым дистанционным способом, на наш взгляд, целесообразно придерживаться точки зрения А. Н. Халикова. Автор именует данный этап постпреступной деятельностью, которая выражается в том числе в противодействии оперативно-розыскной деятельности, направленной на выявление преступлений [8, с. 106].

Основной задачей, решаемой мошенниками на данном этапе, по нашему мнению, является обеспечение доступа к похищенным средствам при условии сохранения собственной анонимности. Выбор пути обеспечения доступа к похищенным средствам непосредственно зависит от ранее реализованного злоумышленниками способа завладения денежными средствами.

Так, в случае передачи потерпевшим наличных денежных средств курьеру последний отправляет деньги куратору путем их перевода на банковский счет; электронный или криптокошелек; наличными – третьему лицу или иным способом. Приоритетным способом является конвертация наличных денежных средств в криптовалюту. В связи с высокой степенью вероятности задержания курьера, замысел организаторов заключается в том, чтобы тот контактировал с денежными средствами минимально возможное время.

При наличии иностранной валюты курьер производит ее обмен на белорусские рубли, а затем, используя различные сервисы и устройства банковского самообслуживания, переводит деньги на счет, реквизиты которого получает от куратора. Это обусловлено тем, что при осуществлении прямого перевода иностранной валюты требуется предоставление персональных данных. Имеется также возможность обмена наличных денежных средств на криптовалюту в ходе личной встречи, что исключает необходимость их зачисления на банковский счет.

В случае, когда мошеннику, вовлеченному в преступную группу, удается заполучить денежные средства жертвы путем онлайн-перевода, они не поступают напрямую к непосредственному исполнителю преступления. Их зачисление производится на БПК, выпущенную на имя «дропа». Следовательно, они находятся под непосредственным управлением кураторов преступной группы, однако поступление денежных средств на БПК посредника не является конечной целью. Переводить их на собственный счет напрямую рискованно с точки зрения нарушения анонимности. При этом стоит учитывать тот факт, что посредник теоретически может получить к ним доступ и, в связи с этим, хранить их длительное время на данном счете небезопасно. Фиатные [1] деньги на личные счета злоумышленники, как правило, переводят, предварительно конвертировав их в криптовалюту. С целью недопущения компрометации криптокошелька, находящегося в личном пользовании, преступники могут использовать криптомиксеры[2].

При распределении денежных средств между соучастниками принимаются меры и по противодействию их идентификации. Один из самых распространенных способов – предоставление ссылки на BTC-чек. Выбор криптовалюты Bitcoin (BTC) обусловлен ее распространенностью и более развитой, в сравнении с аналогами, инфраструктурой. Данный инструмент работает по принципу банковского чека на предъявителя. При переходе по ссылке злоумышленник указывает свой биткоин-кошелек, на который автоматически поступают зарезервированные средства. Таким образом, организаторы и исполнители минимизируют контакты между собой, что создает дополнительные сложности для правоохранительных органов при установлении связей и изобличении конкретных лиц. Выяснить, кто именно создал BTC-чек, очень затруднительно.

Для указанных целей используются боты в мессенджере Telegram. Они являются продуктами криптовалютных бирж, зарегистрированных за пределами Республики Беларусь. В связи с совершенствованием регулирования оборота криптовалют регистрация на большинстве бирж в

[1] Фиатные (от лат. fiat – декрет, указание, «да будет так») – деньги, номинальная стоимость которых устанавливается и гарантируется государством.

[2] Криптомиксер – сервис анонимизации, который существенно усложняет отслеживание транзакций в системе блокчейн.

данный момент предусматривает обязательную верификацию для всех пользователей, но на некоторых из них возможно использование аккаунтов, зарегистрированных без верификации до введения указанного правила. При этом процедура верификации аккаунтов не исключает возможности их создания для последующей продажи «дропами» по аналогии с БПК.

Препятствия для деанонимизации данных пользователей заложены в самом алгоритме проведения транзакции. Отправляя средства по сгенерированному BTC-чеку с целью экономии времени и снижения комиссии за проверку транзакции в блокчейне биржа аккумулирует несколько транзакций в одну и использует кошельки, не имеющие отношения к администратору преступной группы, осуществляющему перевод.

Для вывода денежных средств мошенники, как правило, используют либо «десктопные»[1], либо «холодные»[2] кошельки, не ассоциированные с криптовалютными биржами, что совсем исключает их верификацию. Принадлежность данных кошельков можно установить только по косвенным признакам, однако выяснить даже эти сведения не всегда представляется возможным.

Таким образом, полагаем возможным отметить следующие особенности механизма совершения мошенничеств дистанционным способом:

1. Разработка типовой модели данного вида преступления, не привязываясь к конкретным способам, видится целесообразной. Связано это с тем, что классификация мошенничеств по способу их совершения достаточно затруднительна. Значимость данного подхода для ОРД выражается в подробном описании каждого из этапов исследуемого преступления, что позволит эффективнее устанавливать лиц, причастных к его совершению.

2. В основе формирования механизма мошенничеств, совершенных дистанционным способом, заложены три этапа: начальный, основной, завершающий. Меры по сокрытию следов преступления и сохранению собственной анонимности мошенники принимают на всех трех этапах.

3. Особую роль в реализации механизма описываемого преступления играет начальный этап его совершения. Результаты последующих стадий напрямую зависят от качества произведенных на данном этапе подготовительных действий.

4. В ходе реализации основного этапа мошенники вовлекают жертву в легенду мошенничества и в последующем склоняют ее к непосредственной передаче им денежных средств. Произошедшие на данной стадии изменения в образе действий потерпевшего могут стать препятствием к реализации преступного замысла мошенников.

5. Основная задача мошенников на завершающем этапе – обеспечить доступ к похищенным средствам при условии сохранения собственной анонимности. Выбор пути обеспечения доступа к похищенным средствам непосредственно зависит от ранее реализованного злоумышленниками способа завладения ими.

Список использованных источников

1. Кустов, А. М. Криминалистика и механизм преступления : цикл лекций / А. М. Кустов. – Воронеж : МОДЭК, 2002. – 304 с.

2. Осипенко, А. Л. О характеристике способов совершения сетевых компьютерных преступлений / А. Л. Осипенко // Вестн. криминалистики. – 2009. – № 4. – С. 149–154.

3. Ермолович, Д. В. О механизме мошенничества / Д. В. Ермолович // Вестн. Акад. МВД Респ. Беларусь. – 2004. – № 2. – С. 109–111.

4. Якимов, И. Н. Криминалистика : рук. по уголов. технике и тактике / И. Н. Якимов. – М. : ЛексЭст, 2003. – 471 с.

5. Кузьмин, И. А. Раскрытие мошенничеств, совершенных с использованием информационно-коммуникационных технологий : учеб. пособие / И. А. Кузьмин. – Иркутск : ФГКОУ ВО ВСИ МВД России, 2021. – 80 с.

6. Давидович, Е. И. Структура преступных групп, специализирующихся на совершении мошеннических действий в сети Интернет / Е. И. Давидович // Проблемы борьбы с преступностью и подготовки кадров

[1] Десктопная версия – это версия программного обеспечения, управляемая пользователем после непосредственной установки на средство компьютерной техники.

[2] Холодный кошелек (Ledger) – это физическое устройство или приложение, предназначенное для безопасного хранения и управления криптовалютными активами без постоянного подключения к интернету. В отличие от горячих кошельков, работающих онлайн, холодные кошельки полностью изолированы от сети, что позволяет обеспечить повышенную безопасность средств.

для правоохранительных органов : Междунар. науч.-практ. конф., Минск, 28 янв. 2022 г. : тез. докл./ Акад. М-ва внутр. дел Респ. Беларусь ; редкол.: П. В. Гридюшко (отв. ред.) [и др.]. – Минск, 2022. – С. 101–102.

7. Губич, М. В. Проблемные аспекты определения сущности и содержания социальной инженерии в контексте обеспечения информационной безопасности / М. В. Губич // Вестн. Акад. МВД Респ. Беларусь. – 2022. – № 1. – С. 18–23.

8. Халиков, А. Н. Должностные преступления: характеристика, расследование, предупреждение (криминалистический аспект) : монография / А. Н. Халиков ; под ред. В. И. Комиссарова. – М. : Юрлитинформ, 2012. – 105 с.

Дата поступления в редакцию: 17.03.2023

УДК 343.985

***С. В. Король**, адъюнкт научно-педагогического факультета*
Академии Министерства внутренних дел Республики Беларусь
e-mail: sergey_moz@mail.ru

ИСТОРИЯ СТАНОВЛЕНИЯ НА БЕЛОРУССКИХ ЗЕМЛЯХ ПРАВОВОГО РЕГУЛИРОВАНИЯ ГЛАСНОГО СОДЕЙСТВИЯ ГРАЖДАН ОРГАНАМ, ОСУЩЕСТВЛЯЮЩИМ ОПЕРАТИВНО-РОЗЫСКНУЮ ДЕЯТЕЛЬНОСТЬ ДО ПЕРИОДА ОБРАЗОВАНИЯ СОВЕТСКОГО ГОСУДАРСТВА

Рассматривается развитие и становление института гласного содействия в оперативно-розыскной деятельности (ОРД) в Республике Беларусь. Акцентируется внимание на анализе исторических этапов развития института, определении его места и роли в ОРД в рамках исследуемой темы. Выявляются вопросы, требующие дополнительного научного изучения. С учетом того, что наука ОРД является относительно молодым направлением в юриспруденции Беларуси, принимается во внимание, что история института гласного содействия граждан органам, осуществляющим ОРД, не была подробно теоретически изучена в научных работах. Предлагается провести комплексный ретроспективный анализ правового регулирования ОРД в истории Беларуси.

Ключевые слова: правовое регулирование, гласное содействие, оперативно-розыскная деятельность, история, правоохранительные органы.

***S. V. Korol**, Postgraduate student of the Scientific and Pedagogical Faculty*
of the Academy of the Ministry of Internal Affairs of the Republic of Belarus
e-mail: sergey_moz@mail.ru

HISTORY OF THE DEVELOPMENT OF LEGAL REGULATION OF PUBLIC ASSISTANCE TO THE DETECTIVE AGENCIES ON THE TERRITORY OF BELARUS BEFORE THE SOVIET STATE FORMATION

The article deals with the development and formation of the institute of public assistance in detective activity in the Republic of Belarus. The article focuses on the analysis of historical stages of development of the institute, determination of its place and role in the detective activity within the framework of the topic under study. The issues requiring additional scientific study are identified. Taking into account the fact that the science of detective activity is a relatively young area of law in Belarus, it is taken into account that the history of the institute of public assistance to the detective agencies has not been theoretically studied in detail and considered in scientific works. It is proposed to conduct a comprehensive retrospective analysis of the legal regulation of detective activity in the history of Belarus.

Keywords: legal regulation, public assistance, detective activity, history, law enforcement agencies.

Исследование института гласного содействия в оперативно-розыскной деятельности невозможно без рассмотрения и анализа основных исторических этапов его развития. Указанный подход позволяет изучить место и роль данного специфического института в ОРД, выделить вопросы, не подвергавшиеся ранее доскональному изучению, предложить их решение.

Наука ОРД в Республике Беларусь является достаточно молодым направлением в юриспруденции, и, соответственно, по объективным причинам история развития института гласного со-