YURIDIK FANLAR AXBOROTNOMASI

ВЕСТНИК ЮРИДИЧЕСКИХ НАУК

REVIEW OF LAW SCIENCES

VOLUME 8 / ISSUE 1 / 2024

DOI: 10.51788/TSUL.ROLS.2024.8.1.

ISSN 2181-919X

E-ISSN 2181-1148

DOI: 10.51788/TSUL.ROLS

MUNDARIJA

12.00.08 – JINOYAT HUQUQI. HUQUQBUZARLIKLARNING OLDINI OLISH. KRIMINOLOGIYA. JINOYAT-IJROIYA HUQUQI

12.00.09 – JINOYAT PROTSESSI. KRIMINALISTIKA, TEZKOR-QIDIRUV HUQUQ VA SUD EKSPERTIZASI

E-ISSN 2181-1148
ISSN 2181-919X

DOI: https://dx.doi.org/10.51788/tsul.rols.2024.8.1./UXTW4602
UDC: 343.98(045)(575.1)

НОВЫЕ СПОСОБЫ ОТМЫВАНИЯ ДЕНЕЖНЫХ СРЕДСТВ ПРИ СОВЕРШЕНИИ КИБЕРПРЕСТУПЛЕНИЙ

Сабырбаева Айнура Бахыт кызы.
доцент кафедры уголовно-процессуального права
Академии МВД Республики Узбекистан
ORCID: 0000-0002-8364-5319
e-mail: a_sabyrbaeva@inbox.ru

Аннотация. *В статье рассматриваются современные способы, используемые для отмывания денежных средств, добытых преступным путём при совершении киберпреступлений, а также обосновывается необходимость внесения изменений в действующее уголовное и административное законодательство за передачу банковской карты или номеров сим-карт третьим лицам, в том числе и в отношении самих дропов, так как именно данные инструменты играют ключевую роль в сокрытии следов преступления и отмывании денежных средств. Описывается роль дропов и дроповодов в составе организованной преступной группы, а также преступные схемы, которые используются для нахождения дропов в виртуальной сфере путём размещения рекламы о трудоустройстве (возможность получения «лёгкого» заработка) или нахождения в режиме офлайн (через знакомых, среди лиц с алкогольной зависимостью или лиц без определённого места жительства). Кроме того, в статье рассматриваются виды дропов, или денежных мулов, с приведением примеров об особенностях той или иной категории. Сделан сравнительно-правовой анализ зарубежного законодательства об ответственности за передачу третьим лицам платёжной карты или номера сим-карты (КНР, Франция, Германия), а также практический опыт КНР в противодействии легализации доходов, добытых преступным путём.*

Ключевые слова: *киберпреступность, дроп, дроповод, платёжная карта, отмывание денежных средств, номера сим-карт, уголовная ответственность, мобильные операторы.*

KIBERJINOYATLARNI SODIR ETISHDA PUL MABLAG'LARINI YUVISHNING YANGI USULLARI

Sabirbayeva Aynura Baxit qizi,
O'zbekiston Respublikasi IIV akademiyasi
Jinoyat-protsessual huquqi kafedrasi dotsenti

Annotatsiya. *Maqolada kiber jinoyatlar sodir etishda jinoiy yo'l bilan olingan pullarni legallashtirishda qo'llanadigan zamonaviy usullar ko'rib chiqilgan, shuningdek, droplarga nisbatan bank kartasi yoki SIM-karta raqamlarini uchinchi shaxslarga o'tkazish uchun javobgarlik belgilash va amaldagi jinoiy va ma'muriy qonunchilikka o'zgartirish kiritish zarurligi asoslangan. Aynan shu vositalar jinoyat izlarini yashirishda va jinoyatchilikdan olingan daromadlarni legallashtirishda muhim ahamiyatga ega. Unda uyushgan jinoiy guruhning bir qismi sifatida droplar va dropovodlarning o'rni va vazifalari, shuningdek, droplarni topishning usullari, ya'ni onlayn reklama joylashtirish orqali (ishga joylashish bo'yicha e'lonlar, masalan, "oson" daromad topish) yoki oflayn*

rejim (tanishlar, spirtli ichimliklarni iste'mol qilishga moyil bo'lgan shaxslar, yashash joyi aniq bo'lmagan shaxslar), droplarni topish uchun ishlatiladigan jinoiy sxemalar tasvirlangan. Bundan tashqari, maqolada droplarning turlari va har bir toifaning xususiyatlari misollar bilan keltirilgan. To'lov kartasi yoki SIM-karta raqamini uchinchi shaxslarga o'tkazish uchun javobgarlik to'g'risidagi xorijiy qonunchilikning (Xitoy, Fransiya, Germaniya) qiyosiy-huquqiy tahlili amalga oshirgan, shuningdek, Xitoy Xalq Respublikasining jinoyatchilikdan olingan daromadlarni legallashtirishga qarshi kurashish bo'yicha amaliy tajribasi ko'rib chiqilgan.

Kalit so'zlar: *kiberjinoyatchilik, drop, dropovod, to'lov kartasi, jinoiy daromadlarni legallashtirish, SIM-karta raqamlari, jinoiy javobgarlik, uyali aloqa operatorlari.*

NEW WAYS OF MONEY LAUNDERING IN CYBERCRIMES

Sabirbaeva Ainura Bakhit kizi,
Associate Professor of the Department
of Criminal Procedure Law,
Academy of the Ministry of Internal Affairs
of the Republic of Uzbekistan

Abstract. *The article considers modern methods used for laundering criminally obtained funds in the course of committing cybercrimes, and substantiates the necessity to amend the current criminal and administrative legislation for transferring bank card or SIM card numbers to third parties as for the droppers themselves. Since these tools play a key role in hiding traces of crime and money laundering. The article describes the role of droppers and droppers as part of an organized criminal group, as well as criminal schemes that are used to find droppers in the virtual sphere by placing advertisements for employment (obtaining "easy" earnings) or by finding them offline (through acquaintances, among persons with alcohol addiction or persons of no fixed abode). In addition, the article discusses types of dropships or money mules with examples of peculiarities of this or that category. A comparative legal analysis of foreign legislation on liability for the transfer of payment card or SIM card number to third parties (PRC, France, Germany) is made, as well as the practical experience of the PRC in combating money laundering.*

Keywords: *cybercrime, dropping, dropper, payment card, money laundering, SIM card numbers, criminal liability, mobile operators.*

Введение

Ни для кого ни секрет, что преступники день ото дня совершенствуют свои методики и способы для облегчения совершения преступлений, в том числе и киберпреступники, которые для достижения своих преступных целей используют не только IT-навыки, программирование, (де)шифрование, социальную инженерию, но и имеющиеся лазейки в законе. Киберпреступность давно перешагнула порог от совершения кибератак в одиночку, в режиме alone до создания целых организованных преступных групп. К этому процессу также подключились и те, кто раньше осуществлял все преступные замыслы в офлайн-режиме, к примеру наркоторговцы, торговцы оружием и т. д.

Возможности глобальной сети Интернет, в том числе и Darknet, поражают. В Darknet можно не только приобрести наркотики, конфиденциальные данные клиентов банков или платёжных систем, софт для осуществления кибератаки, так и набрать команду для осуществления той или иной преступной схемы в виртуальном пространстве (coder, topic starter, vbiver, scammer и т. д.). Объеди-

нение в команду особенно крайне важно в киберпреступлениях, связанных с завладением чужими денежными средствами, так как каждый член организованной группы выполняет определённую роль. Одним из важнейших членов данной группировки является тот, кто помогает сокрыть следы преступления и отмыть денежные средства, чтобы не попасться в сети правоохранительных органов. Его именуют по-разному: в европейских странах – money mull (денежный мул), у нас – дроп.

Проанализированные данные показывают, что за денежным мулом стоят не мелкие преступники, а сложные преступные организации, вопреки ожидаемому. Как выразился президент Евроюста Джон Лейден (John Leyden): «Важно понимать, что отмывание денег на первый взгляд может показаться мелким преступлением, но оно организовано организованными преступными группами» [1]. Однако, к сожалению, роль дропов или денежных мулов остаётся в значительной степени неисследованной, как для IR, так и для социальных наук [2].

Следует отметить, что появление термина «отмывание денег» для обозначения процесса преобразования денег, полученных преступным путём, в имущество, имеющее вид правомерно полученного, часто связывают с деятельностью известного чикагского гангстера Аль Капоне. Согласно распространённой версии, денежные средства, получаемые от бутлегерства – контрабанды алкоголя в период действия так называемого «сухого закона» в США, для введения в легальный оборот смешивались с выручкой принадлежавшей Аль Капоне сети прачечных самообслуживания [3]. Таким образом происходило отмывание «грязных» денег и их «обеление». Хотя в юридическом и законодательном контексте это выражение впервые появилось в США в 1982 году.

Сегодня опасность киберпреступлений связана с тем, что поймать преступника и выследить его очень трудно, так как используются современные технологии, такие как VPN-сервис (при использовании платной версии стоимостью от 500 долларов США найти местоположение преступника практически нереально). К тому же для отмывания денег обязательно нужен человеческий капитал – дропы.

Дроп, или денежный мул, которого иногда называют «смурфером», это человек, который переводит деньги, полученные незаконным путём, например путём кражи или мошенничества. Денежные мулы переводят средства лично, через курьерскую службу или в электронном виде от имени других [4]. Дропы – это те, кого используют преступники, скорее, как «расходный материал», потому что именно на них сотрудники правоохранительных органов выходят в первую очередь. Данного мнения придерживается и ряд европейских учёных [5].

По мнению Рэнер Халс (Rainer Hulsse), «Преступники обычно нанимают денежных мулов в западных странах, чтобы им не приходилось переводить украденные деньги непосредственно на свои собственные банковские счета, поскольку это значительно облегчило бы правоохранительным органам выявление бенефициаров» [6, с. 1008].

Банки, в которых открываются счета денежных мулов, чтобы снять с себя ответственность, придумали теорию securitisation (т. е. объявляются представляющими угрозу безопасности), утверждая, что денежные мулы подвергаются секьюритизации [7, с. 415].

Материалы и методы

В ходе исследования широко использовались методы познания: анализа, синтеза, логики, сравнительно-правового анализа, наблюдения, обобщения, системного анализа, опроса. Кроме того, были изуче-

E-ISSN 2181-1148
ISSN 2181-919X

ны материалы уголовных дел, расследуемых в Отделе по борьбе с преступлениями в сфере информационных технологий ОБПСИТ ГУВД города Ташкента, а также приговоров, вынесенных судами города Ташкента в отношении лиц, совершивших киберпреступления. Также был проведён опрос среди следователей и дознавателей по поводу необходимости внесения изменений в уголовное и административное законодательство за передачу банковской платёжной карты или номера сим-карты третьим лицам (дропам).

Результаты исследования

Преступная схема такова, что дроповоды (организуют деятельность дропов) находят дропов либо в онлайн-, либо в офлайн-режиме.

В онлайн-режиме дропов находят через социальные сети (Telegram, Instagram, Facebook) путём выкладывания объявлений подобного рода («Хотите заработать деньги быстро и без усилий? Опыт не требуется! Только желание заработать!» и т. д.). Уровень грамотности авторов данных объявлений – дроповодов очень низкий. Как верно отметил в своём исследовании Брук С. Чарльз (Brooke S. Charles): «Тем не менее их образование, по-видимому, базовое, учитывая плохой язык в их электронных письмах о приёме на работу» [8].

После размещения рекламы и объявлений с дроповодами связываются потенциальные дропы. Как отметили некоторые учёные, денежных мулов вербуют с использованием различных подходов, часто заманивая обещаниями роскошного образа жизни, чтобы заинтересовать потенциальных денежных мулов [7]. На данную удочку в основном попадаются лица с низким уровнем образования либо с низкой финансовой грамотностью, так как любой грамотный человек понимает, что «бесплатный сыр бывает только в мышеловке» и получить работу за 10 тыс. долларов США, не прилагая никаких усилий, нереально.

Стоит отметить, что существует несколько видов дропов. ФБР делит денежных мулов на три категории в зависимости от их целей и степени вовлечённости: неосведомлённые денежные мулы; сознательные денежные мулы; денежные мулы – соучастники [9].

Дропы первой категории не знают, что с их помощью совершается сокрытие следов преступления. Так, по уголовному делу № 1-1003-2204/773 [10], граждане Ю. и Э., по предварительному сговору с группой лиц, занимались тем, что находили дропов, в основном в офлайн-режиме среди знакомых и родственников (последние не знали о том, что их конфиденциальные данные похищены), чьи платёжные карты в последующем использовались для отмывания денег. За каждую платёжную карту дроповоды получали 20 долларов США.

Вторая категория дропов: они сами связываются с дроповодами и продают свои платёжные карты или номера симкарт дроповодам за определённую сумму денег. В социальной сети Telegram существует множество групп, в которых продаются и приобретаются подобные услуги. Для совершения данного преступления дроповоды требуют выполнить его инструкции, заключающиеся в том, чтобы оформить платёжную карту определённого банка и через банкомат подключить смс-информирование на указанный дропом телефонный номер. После этого дроп должен сломать физическую карту. Весь этот процесс сопровождается видеофиксацией. После выполнения данных требований дропу на указанную им карту скидывается обговоренная сумма денег (от 20 тыс. до 3 млн сумов в зависимости от количества, типа платёжной карты (VISA, HUMO, UzCard) и банка, в котором открыт банковский счёт). Следует отметить, что

даже при выявлении дропа выйти на дроповода в данном случае практически невозможно, так как не было физического контакта, аккаунт открыт на купленные на специальных платформах виртуальные номера, телефонный номер, который использовался для привязки карты, также был куплен в данных социальных сетях, и деньги переведены на счёт дропа с карты другого дропа.

Согласно отчёту правоохранительных органов Швеции, становится проблемой найти достаточно наивных людей, согласных стать дропами [11, с. 41], однако, как показывает анализ изучения уголовных дел, в каждом случае совершения вишинга преступниками использовались карты дропов [12].

Возникает вопрос зачем нужны карты дропов? Они играют ключевую роль в том, чтобы истинные преступники оставались в тени. Сначала они осуществляют киберпреступление, к примеру фишинг или вишинг, после чего похищенные денежные средства направляются на счёт карт-дропов. На карте дропов деньги остаются не более часа, они немедленно перекидываются на несколько карт дропов, а потом через электронные кошельки или крипто биржи выводятся на зарубежные счета. После получения сведений, составляющих банковскую тайну, естественно, сотрудники выходят на дропов, но у тех есть ответ: до этого они продали свои карты за определённую сумму.

Третья категория дропов – те, кто в курсе того, что благодаря им отмываются деньги, добытые преступным путём. Но, несмотря на это, за каждую транзакцию и перевод через его карту они получают вознаграждение. Так, по уголовному делу № 1–1007–2201/253, гражданка Н. в мессенджере Telegram, вступив в преступный сговор с неизвестным лицом с никнеймом «Mercedes» и обговорив заведомо преступный план хищения денежных средств с банковских пластиковых карт граждан с условием получения 3 % от украденной суммы, предоставила данному лицу доступ к своим банковским пластиковым картам с целью транзита украденных средств через её банковские пластиковые карты на кошельки платёжного сервиса QIWI. В данном конкретном случае она была привлечена к уголовной ответственности по статье 243 УК.

Однако первую и вторую категорию дропов привлечь к уголовной ответственности практически невозможно в связи с тем, что в национальном законодательстве не предусмотрена уголовная ответственность за продажу и передачу третьему лицу банковской карты, что является главным инструментом и лазейкой при отмывании денег. Привлечь дропа как соучастника по статье 243 УК возможно, но только после допроса дроповода, который и должен указать, знал дроп об источнике поступавших на его счёт денег или нет, а, учитывая сложную схему по вербовке дропа, изобличить дропа таким образом очень сложно. Во-первых, понимание того, что денежный мул является невинной жертвой, в значительной степени исключает применение к нему жёстких мер. Как было отмечено в отчётах швейцарского Подразделения финансовой разведки Швейцарии, большинству денежных мулов сходит с рук отсутствие штрафов, или они отделываются только небольшим штрафом из-за трудности доказать, что мул осведомлён о преступлении [13].

Дропов в офлайн-режиме ищут, как правило, среди алкоголиков, бомжей, в студенческих общежитиях и многолюдных местах, где за определённую сумму денег их просят оформить в ближайшем банке платёжную карту или номер сим-карты, чтобы сразу пройти онлайн-идентификацию в мобильном приложении для последующего осуществления транзакции. В проведённом исследовании

в Малайзии было установлено, что синдикаты обычно получают счета денежных мулов (также известные как суррогатные счета) путём обмана тех, кто нуждается в дополнительном доходе и имеет низкий уровень финансовой грамотности [14, с. 481]. Это не только лица престарелого возраста, но и молодые люди.

Не только банковская карта, но и номер сим-карты также является основным предметом сделок между дропами и дроповодами, так как для осуществления регистрации в мобильных приложениях и транзакции необходима привязка банковской платёжной карты к номеру сим-карты. Однако схема приобретения сим-карт немного отличается от получения банковских карт, так как дроповодам в данном случае нужны физические сим-карты, которые он должен получить от дропа. Так, дропов просят оформить на себя сим-карты, желательно несколько (в РФ, к примеру, правоохранительными органами у одного дропа было изъято 1 608 карт [15]), оставить физические сим-карты в определённом месте, скинуть локацию, чтобы избежать реального контакта с дроповодом (аналогичная схема действует и для закладчиков наркотических средств). После выполнения инструкции дропу скидываются денежные средства на указанную им карту.

Номера телефонов сим-карт используются не только для привязки банковской карты, но и для осуществления полноценной транзакции посредством услуги «Мобильный платёж» (фактически она сама выполняет роль платёжной карты), похищенные денежные средства перенаправляются на другие телефонные номера дропов, а потом через электронные кошельки или криптобиржу, к примеру Binance осуществляются P2P переводы для покупки криптоактивов через обменщиков и, направляя деньги на «горячий» кошелёк самой платформы (Hot Binance), переводятся на другие криптокошельки.

Хотя в правилах использования сервиса «Мобильный платёж», к примеру мобильного оператора Билайн, установлена возможность не исполнения или приостановления оператором распоряжения о переводе денежных средств, «при возникновении у оператора оснований полагать, что существует риск направления несанкционированного Распоряжения и/или нарушения требований законодательства Республики Узбекистан в области противодействия легализации (отмыванию) доходов, полученных преступным путём, и финансирования терроризма. Но обязательным условием является уведомление об этом абонента посредством направления SMS-сообщения или иным способом» [16]. Это, естественно, может привести к тому, что абонент будет стараться быстрее перевести денежные средства через другие сервисы, чтобы сохранить оставшуюся часть похищенных средств. «При использовании Абонентом “электронного счета” для накопления денежных средств (суммы, превышающей среднемесячную абонентскую плату за тарифный план в 20 раз и более), в том числе полученных от третьих лиц, Оператор оставляет право применять штрафную санкцию в размере 4,5 % от суммы денежных средств, подлежащих возврату абоненту, либо обратиться в уполномоченные государственные органы, участвующие в противодействии легализации доходов, добытых преступным путём». В целях выполнения требований законодательства Республики Узбекистан в области противодействия легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма мобильные операторы обязаны осуществлять действия и/или запрашивать информацию у абонента при оказании услуг в пределах сервиса «Мобильный платёж» [16]. Хотя, как показы-

вает практика, данную обязанность они вряд ли выполняют.

Так, по уголовному делу № 260001/2023-1099ПН у преступника Т. была изъята 71 сим-карта (из них 64 – мобильного оператора Билайн), принадлежащая разным мобильным операторам, зарегистрированная на разных лиц, которые оказались дропами (продали сим-карты за определённую сумму денег). Целью преступника было отмывание похищенных денежных средств с помощью данных сим-карт и дальнейшее направление денежных средств на различные международные электронные кошельки. 200 раз осуществлялись переводы денежных средств на счета сим-карт на общую сумму 200 млн сумов (каждый перевод по 1 млн). Несмотря на явную легализацию доходов, добытых преступным путём, мобильные операторы не предприняли никаких действий для блокировки данных абонентов, что привело к отмыванию достаточно крупной суммы.

Закон Республики Узбекистан «О противодействии легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения» от 2004 года № 660-II гласит, что «к организациям, осуществляющим операции с денежными средствами или иным имуществом, также относятся организации, осуществляющие денежные переводы, платежи и расчёты (в том числе и мобильные операторы)… Организации, осуществляющие операции с денежными средствами или иным имуществом, обязаны: организовывать и внедрять системы внутреннего контроля, осуществлять процедуры идентификации и принимать меры по надлежащей проверке клиентов, в том числе верификацию и регулярное обновление данных о клиенте и их собственниках; *идентифицировать собственников* и лиц, контролирующих клиентов, а также *принимать доступные меры по проверке их личности*».

Однако, несмотря на то, что номера сим-карт выступают в качестве орудия по «отмыванию» доходов, добытых преступным путём, являются необходимым условием для привязки банковской платёжной карты и использования интернет-банкинга, не применяется никакая ответственность в отношении мобильных операторов и банковских учреждений, а также лиц, продавших данные номера сим-карт.

Согласно проведённому опросу среди следователей и дознавателей, 100 % респондентов выступили за необходимость введения административной и уголовной ответственности за передачу третьим лицам банковской платёжной карты и номеров сим-карт.

Статистика показывает, что средний возраст дропов составляет 18–25 лет [17]. По данным European Money Mule Actions, дропами чаще всего становятся мужчины; молодые люди от 18 до 34 лет [18]. В Голландии был проведён онлайн-опрос среди более чем 3 тыс. человек в возрасте от 16 до 25 лет, который показал, что около 10 % из них предлагали стать дропами как через социальные сети Snapchat и Instagram, так и в офлайн-режиме (сверстники в школе, знакомые, друзья) [19]. Менее 1 % признались, что в действительности были денежным мулом, а некоторые и вовсе посчитали приемлемым передать свои карты для использования третьими лицами [20]. Именно из этой категории лиц и вербуют дропов для последующего отмывания похищенных денежных средств.

Как справедливо отметила Е. Шестернёва, «кредитные организации обязаны разрабатывать правила внутреннего контроля, назначать специальных должностных лиц, ответственных за реализацию правил внутреннего контроля, а также

E-ISSN 2181-1148
ISSN 2181-919X

принимать иные внутренние организационные меры в указанных целях» [21, с. 30]. Такое правило есть в уставах всех коммерческих банков, однако на деле наблюдается иное. Так, при изучении материалов уголовных дел было установлено, что внутренняя проверка проводится банками только в случае кражи денежных средств непосредственно со счетов банка (взлом серверов).

Стоит отметить, что в КНР установлен лимит предоставления номеров сим-карт на одно лицо, а именно: не более четырёх. В случае если лицо передаст их третьим лицам, то он будет привлечён к ответственности. Иностранным гражданам предоставляется один номер сим-карты, функционирующий 30 дней. Данная практика позволяет пресечь использование карт дропов. Другим положительным опытом КНР является невозможность осуществления трансграничных переводов через банковские карты или банкоматы, необходимо лично обратиться в банковское учреждение, что резко повышает шансы в борьбе с отмыванием доходов, добытых преступным путём.

Исходя из вышеизложенного, предлагается ввести *лимит на предоставление номеров сим-карт на одного человека* для пресечения деятельности дропов и легализации доходов, добытых преступным путём.

Учитывая, что легализация доходов, добытых преступным путём, осуществляется не только с помощью банковских платёжных карт, но и номеров SIM-карт, целесообразно дополнить Кодекс Республики Узбекистан об административной ответственности статьей 179[6] и изложить её в следующей редакции:

«Нарушение порядка предоставления операторами сотовой связи номеров SIM-карт

Нарушение порядка предоставления операторами сотовой связи номеров SIM-карт, в том числе без истребования, получения или идентификации личности, приведшее к последующей передаче данных номеров SIM-карт третьим лицам, а также превышение лимита оформленных на одно лицо номеров SIM-карт, —

влечёт наложение штрафа от пятидесяти до ста базовых расчётных величин».

Наказания за добровольное предоставление средств платежа мошенникам существуют и весьма суровые. Скажем, в Китае наказание может быть пожизненным (в РФ точно так же, в случаях если дроп замешан в переводе средств, направленных на финансирование терроризма). В Европе – до 10 лет заключения [22]. Статья 222 УК Республики Беларусь предусматривает уголовную ответственность за незаконный оборот средств платежа и (или) инструментов: за «… совершённое из корыстных побуждений незаконное распространение реквизитов банковских платёжных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным кошелькам» вплоть до 10 лет лишения свободы, а административной ответственности за это не предусмотрено.

В Тайване [23] 19 мая 2023 года были внесены поправки в Закон «О борьбе с отмыванием доходов», предусматривающие дропам уголовную ответственность. Статья 15-1 Закона указывает: «Ни одно лицо не должно передавать или предоставлять доступ другой стороне к информации об учётной записи, которую он или она или другие лица подали в финансовое учреждение, или к номеру счета, который он или она подали в компании, занимающиеся платформами виртуальной валюты или транзакциями, или к номерам счетов, поданным в сторонние платёжные сервисы. Лицо подлежит наказанию в виде тюремного заключения на срок до трёх лет, содержания под стражей и/или штрафа в размере до одного миллиона новых тай-

ваньских долларов, если: 1) преступление совершено во время дачи обещаний или услуги за услугу; 2) общее количество счетов или доставленных номеров счетов больше трёх; 3) преступление совершено повторно в течение пяти лет после первого выговора со стороны полицейских властей».

Если пользователь просто передаёт свою банковскую карту с паролем или предоставляет номер карты, чтобы ему перевели денежные средства, – эти действия не являются уголовно наказуемыми и считаются законными, поскольку они ограничиваются лишь его личными платежами и не затрагивают чужие интересы.

Статья 191 УК КНР [24] предусматривает уголовную ответственность за содействие в переводе денежных средств путём перечисления на счёт или путём использования иных способов расчёта; содействие в переводе денежных средств за границу; утаивание и сокрытие иными способами источников и характера доходов, полученных преступным путём, квалифицируя данные деяния как отягчающее обстоятельство (наказывается до 10 лет лишения свободы и штрафом в размере от 5 до 20 % «отмытых денег».

Согласно статье 324-1 УК Франции [25]: «Отмывание денег – это содействие любым способом ложному обоснованию происхождения имущества или доходов лица, совершившего уголовное преступление или мелкое правонарушение, которое принесло ему прямую или косвенную выгоду. Отмывание денег также включает в себя *содействие* в инвестировании, сокрытии или конвертации прямых или косвенных результатов уголовного преступления или мелкого правонарушения. Отмывание денег наказывается тюремным заключением сроком на пять лет и штрафом в размере 375 тыс. евро».

Согласно статье 261 УК ФРГ [26]: «Любой, кто прячет предмет, являющийся результатом незаконного деяния (тяжкие преступления; мелкие правонарушения в соответствии с (a) разделом 332(1), также в сочетании с подразделом (3) и разделом 334; (b) статья 29 (1) № 1 Закона о наркотиках и статья 19 (1) № 1 Закона о прекурсорах наркотиков (контроле)), скрывает его происхождение или препятствует или *ставит под угрозу расследование* его происхождения, его обнаружение, конфискацию, лишение свободы или официальное обеспечение его сохранности, подлежит тюремному заключению на срок от трёх месяцев до пяти лет. Любое лицо в случаях, предусмотренных подразделами (1) или (2) выше, *по грубой небрежности не осведомлённое* о том факте, что объект является результатом незаконного деяния, указанного в подразделе (1) выше, *подлежит наказанию* в виде тюремного заключения на срок не более двух лет или штрафа». То есть незнание о том, что переведённые через его карту денежные средства были преступными доходами, не освобождает от уголовной ответственности.

В соответствии с законодательством Великобритании дропы могут получить наказание вплоть до 14 лет лишения свободы. Помимо этого, у дропов возникнут проблемы, связанные с получением кредитов или займов, закрытием банковского счета, который использовался в качестве средства по отмыванию денежных средств. Кроме того, в США дропы могут привлечены к персональной ответственности за возврат похищенных у жертв средств, если их карты использовались в качестве средства по отмыванию денежных средств.

Одед Лбвенхейм (Oded Lbwenheim) также утверждал, что «суверен не исключает ответственности за отмывание денег с помощью денежных мулов. Каждый гражданин несёт ответственность за свои поступки и, следовательно, должен быть настороже. В литературе, вдохновлённой

Фуко, такое поведение известно, как "ответственность" (responsibilization), технология управления на расстоянии, которая типична для нашей нынешней государственности» [27, 28].

Как справедливо отметила Лиз Зиглер, директор по потребительскому мошенничеству и финансовым преступлениям Lloyds Bank: «За всеми этими очевидными схемами быстрого обогащения стоят организованные преступные группировки, отчаянно пытающиеся отмыть украденные ими наличные, часто у невинных жертв мошенничества. Вот почему наказания за то, что вы становитесь денежным мулом (money mule), настолько суровы и могут включать тюремное заключение» [29].

Отсутствие в национальном законодательстве ответственности за передачу платёжной карты или номера сим-карты преступникам и за оказание им других услуг приводит к соблазну заработать «лёгкие» деньги, злоумышленники остаются безнаказанными, а денежные средства жертв утекают на зарубежные счета, поэтому не удаётся обеспечить возмещение им материального ущерба.

Выводы

Основной лазейкой в законодательстве, которое и приводит к массовой вербовке дропов, является отсутствие ответственности. Ведь что не запрещено – то разрешено. Поэтому для предотвращения ухудшения криминогенной ситуации целесообразно внести изменение в законодательство, предусматривающее уголовную ответственность за подобное деяние. В связи с этим необходимо внести изменения в действующее административное и уголовное законодательство, чтобы уменьшить количество дропов и предотвратить утечку денежных средств на зарубежные счета.

Дополнить Кодекс Республики Узбекистан об административной ответственности статьёй 179^6 и изложить её в следующей редакции:

«Незаконный оборот средств платежа и (или) инструментов, а также номеров SIM-карт

Передача, приобретение, использование чужих банковских платёжных карт, банковских счетов и счетов на мобильных приложениях, иных платёжных инструментов и средств, номеров SIM-карт и (или) предоставление доступа к нему, а равно незаконное распространение реквизитов банковских платёжных карт, номеров SIM-карт либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным криптокошелькам, —

влечёт наложение штрафа от пятидесяти до ста базовых расчётных величин, или административный арест до пятнадцати суток.

То же правонарушение, повлёкшее причинение значительного ущерба, —

влечёт административный арест до пятнадцати суток с наложением штрафа от ста до ста пятидесяти базовых расчётных величин».

Дополнить Уголовный кодекс Республики Узбекистан статьёй 243^1 и изложить её в следующей редакции:

«Незаконный оборот средств платежа и (или) инструментов, а также номеров SIM-карт

Передача, приобретение, использование чужих банковских платёжных карт, банковских счетов и счетов на мобильных приложениях, иных платёжных инструментов и средств, номеров SIM-карт и (или) предоставление доступа к нему, а равно незаконное распространение реквизитов банковских платёжных карт, номеров SIM-карт либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным криптокошелькам, совершённое после применения административного взыскания за такие же действия, —

наказываются штрафом от ста пятидесяти до трёхсот базовых расчётных величин или исправительными работами от двух до трёх лет либо лишением свободы до трёх лет.

Те же действия, совершённые:

а) по предварительному сговору группой лиц;

б) совершённые повторно или опасным рецидивистом;

в) повлёкшие причинение крупного ущерба,

— наказываются ограничением свободы от трёх до пяти лет или лишением свободы на срок от трёх до десяти лет со штрафом в размере от трёхсот до пятисот базовых расчётных величин.

Те же действия, совершённые:

а) организованной группой или в её интересах;

б) повлёкшие причинение ущерба в особо крупном размере,

— наказываются лишением свободы от пяти до десяти лет лишения свободы».

Кроме того, надо обязать все банковские учреждения при выдаче банковской платёжной карты (физической или виртуальной) предупреждать о наличии ответственности за передачу карты третьему лицу, такую же процедуру сделать обязательной и для мобильных операторов, которые должны предупредить об административной и уголовной ответственности за передачу третьему лицу номеров симкарт.

REFERENCES

1. Leyden J. 178 Arrested in Pan-European Money Mule Crackdown. The Register, 2016, Nov. 22. Available at: http://www.theregister.co.uk/2016/11/22/European_money mule-crackdown

2. Sharman J.C. Power and Discourse in Policy Diffusion: AntiMoney Laundering in Developing States. *52 INT'L STUD. Q.*, 2008, p. 635. Available at: http://www.jstor.org/stable/pdfl29734254.pdfref reqid=excelsior:445177bdc354bd9a264 da04llb4e7Od8&seq=1#page-scantab-contents

3. FAQ. Official website of the Eurasian Group on Combating Money Laundering and the Financing of Terrorism. Available at: https://eurasiangroup.org/ru/faq

4. Money mule. From Wikipedia, the free encyclopedia. Available at: https://en.wikipedia.org/wiki/Money_mule#:~:text=A%20money%20mule%2C%20sometimes%20called,part%20of%20the%20money%20transferred

5. Aston M., McCombie S., Reardon B., Watters P. A Preliminary Profiling of Internet Money Mules: An Australian Perspective. Cybercrime Research Lab, Macquarie University, 2009, DOI: 10.1109/UIC-ATC.2009.63

6. Hulsse R. The Money Mule: its discursive construction and the implications. *50 Vanderbilt Law Review*, 2021, p. 1007. Available at: https://scholarship.law.vanderbilt.edu/vjtl/vol50/iss4/5

7. Vicek W. Securitizing money to counter terrorist finance: some unintended consequences for developing economies, *16 INT'L STUD. PERSP.*, 2015, pp. 406, 414–416.

8. Charles B.S. The most common schemes for targeting the unknowing money mule. *Security Intelligence,* 2014, Sep. 16. Available at: https://securityintelligence.com/the-most-common-schemes-for-targeting-theunknowing-money-mule/

9. What is a Money Mule? Sanction Scanner – Anti-Money Laundering solutions provider. Available at: https://sanctionscanner.com/knowledge-base/money-mules-248

10. Jinoyat ishlari bo'yicha sudlar tomonidan internet tarmog'ida e'lon qilingan sud qarorlari [Court decisions published by courts in criminal cases on the Internet]. Court decisions published on the Internet. Supreme Court of the Republic of Uzbekistan, 2024. Available at: https://public.sud.uz/report/CRIMINAL

E-ISSN 2181-1148
ISSN 2181-919X

11. Melani, information security. Situation in Switzerland and internationally. *Half-year report*, 2016, January-June, vol. 1, p. 41. Available at: https://www.melani.admin.ch/melani/... Ihalbjahresbericht-2016-1.html

12. Analysis of criminal cases being processed by the OBPSIT of the city of Tashkent. 2024.

13. MROS, Annual Report by the Money Laundering Reporting Office Switzerland. *MROS-2014, Federal Office of Police*, 2015, pp. 41–49.

14. Rani M.I.A., Nazri Sh.N.F.S.M., Zolkaflil S. A systematic literature review of money mule: its roles, recruitment and awareness. *Journal of Financial Crime,* 2023, January 5. ISSN: 1359-0790.

15. Droper ponevole: kak ne stat' souchastnikom moshennicheskoy skhemy s bankovskimi kartami [Dropper performedly: how to not become a participant in a fraudulent scheme with bank cards]. HSE Daily is the university brand media of the Higher School of Economics. Available at: https://daily.hse.ru/post/1340

16. Rules for using the Mobile Payment Service. Beeline Uzbekistan official website. Available at: https://beeline.uz/ru/mobilniy-platej

17. An online survey conducted among employees of the Office for Combating Crime in the Sphere of Information Technology. 2024.

18. Ne stanovis' dropom! – besplatnyy syr byvayet tol'ko v myshelovke [Don't become a drop! – free cheese only comes in a mousetrap]. Ukrainian Interbank Association of Members of EMA Payment Systems. Available at: https://www.ema.com.ua/citizens/cyber-safety-school/do-not-become-a-drop-free-cheese-is-only-in-a-mousetrap/

19. Ilyas I.Y., Ridzuan A.R., Mohideen R.S., Bakar M.H. Level of Awareness and Understanding towards Money Mule Among Malaysian Citizens. *Journal of Accounting and Finance in Emerging Economies,* 2022, vol. 8 (4), pp. 481–488.

20. Bekkers L., Van Houten Y., Spithoven R., Leukfeldt E.R. Money Mules and Cybercrime Involvement Mechanisms: Exploring the Experiences and Perceptions of Young People in the Netherlands. 2023, March 30, pp. 1368–1385.

21. Shesterneva Ye. Banki smogut blokirovat' somnitel'nyye platezhi [Banks will be able to block dubious payments]. *Administrative Law,* 2018, no. 3, pp. 29–32.

22. Syemov M. Ot peremeny nazvaniy sroki ne menyayutsya [Changing the names does not change the terms]. *National Banking Journal (NBJ)*. Available at: https://nbj.ru/fingramotnost/ekspert-maksim-syemov-vvedenie-ugolovnogo-/62840/

23. Money Laundering Control Act CH. Amended Date 2023, June 14. Ministry of Justice. Available at: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380131

24. Criminal Code of the People's Republic of China. Amended Date 2016, January, 11. Official website of the Embassy of the People's Republic of China in the Russian Federation. Available at: http://ru.china-embassy.gov.cn/rus/zfhz/zgflyd/201601/t20160111_3149373.htm

25. Penal Code. With the participation of J. Rason. SPENCER QC. University of Cambridge. Selwyn College. 1st part, enacted parts. Available at: https://www.equalrightstrust.org/ertdocumentbank/french_penal_code_33.pdf

26. Golovnenkov P.V. Criminal law of the Federal Republic of Germany – Strafgesetzbuch (StGB). Scientific and practical commentary and translation of the text of the law. Universitätsverlag Potsdam. *Schriften zum deutschen und russischen Strafrecht.* Available at: https://www.uni-potsdam.de/fileadmin/projects/ls-hellmann/Forschungsstelle_Russisches_Recht/Neuauflage_der_kommentierten_StGB-%C3%9Cbersetzung_von_Pavel_Golovnenkov.pdf

27. Lbwenheim O. The responsibility to responsibilize: foreign offices and the issuing of travel warnings. *1 INT'L POL. Soc.,* 2007, pp. 203, 214–215.

28. Sending O.J., Neumann I.B. Governance to Governmentality: Analyzing NGOs, States, and Power. *50 INT'L STUD. Q.*, 2006, pp. 651, 657–658.

29. Ziegler L. Money mules are getting older. Lloyds Bank. Available at: https://www.lloydsbankinggroup.com/media/press-releases/2022/lloyds-bank/money-mules-are-getting-older.html

YURIDIK FANLAR AXBOROTNOMASI
ВЕСТНИК ЮРИДИЧЕСКИХ НАУК
REVIEW OF LAW SCIENCES

Huquqiy ilmiy-amaliy jurnal

Правовой научно-практический журнал

Legal scientific-practical journal

VOLUME 8 / ISSUE 1 / 2024
DOI: 10.51788/TSUL.ROLS.2024.8.1.

BOSH MUHARRIR:
Rustambekov Islambek Rustambekovich
Toshkent davlat yuridik universiteti rektori v.v.b., y.f.d., professor

BOSH MUHARRIR O‘RINBOSARI:
Xodjayev Baxshillo Kamolovich
Ilmiy ishlar va innovatsiyalar bo‘yicha prorektor, y.f.d., professor

Mas’ul muharrir: O. Choriyev
Muharrirlar: Y. Yarmolik, Y. Mahmudov, E. Mustafayev
Musahhih: M. Sharifova
Texnik muharrirlar: U. Sapayev, D. Rajapov

Tahririyat manzili:
100047. Toshkent shahar, Sayilgoh ko‘chasi, 35.
Tel.: (0371) 233-66-36 (1169)

Veb-sayt: review.tsul.uz
E-mail: reviewjournal@tsul.uz
Obuna indeksi: 1385.

Jurnal 26.03.2024-yilda tipografiyaga topshirildi. Qog‘oz bichimi: A4.
Shartli 12,32 b.t. Adadi: 100. Buyurtma raqami: 38.
TDYU tipografiyasida chop etildi.