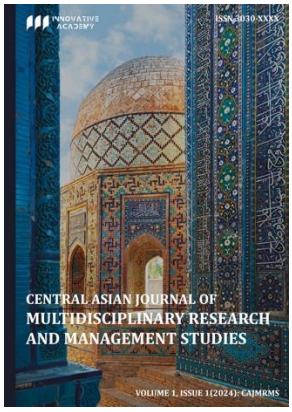

ДРОПЫ КАК СВЯЗУЮЩЕЕ ЗВЕНО ОРГАНИЗОВАННОЙ ГРУППИРОВКИ И СРЕДСТВО ДЛЯ ОТМЫВАНИЯ ДЕНЕЖНЫХ СРЕДСТВ, ДОБЫТЫХ ПРИ СОВЕРШЕНИИ КИБЕРПРЕСТУПЛЕНИЙ

Сабырбаева Айнура Бахыт кызы
доцент кафедры уголовно-процессуального права
Академии МВД Республики Узбекистан
ORCID: 0000-0002-8364-5319
a_sabyrbaeva@inbox.ru
телефон: +99877-007-75-67
https://doi.org/10.5281/zenodo.11524138

ARTICLE INFO

Received: 01st June 2024
Accepted: 03th June 2024
Published: 06th June 2024

KEYWORDS

киберпреступность, дроп, дроповод, платежная карта, отмывание денежных средств, номера SIM-карт, уголовная ответственность, мобильные операторы

ABSTRACT

в статье рассматриваются современные способы, используемые для отмывания денежных средств, добытых преступным путем при совершении киберпреступлений, а также обосновывается необходимость внесения изменений в действующее уголовное и административное законодательство за передачу банковской карты или номеров SIM-карт третьим лицам как в отношении самих дропов. Так как именно данные инструменты играют ключевую роль для сокрытия следов преступления и отмывания денежных средств. Описывается роль дропов и дроповодов в составе организованной преступной группировки, а также преступные схемы, которые используются для нахождения дропов в виртуальной сфере путем размещения реклам о трудоустройстве (получение «легкого» заработка) или путем нахождения в режиме офлайн (через знакомых, среди лиц, с алкогольной зависимостью или лиц без определенного 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 платежной карты или номера SIM-карты (КНР, Франция, Германия), а также практический опыт КНР в противодействии легализации доходов, добытых преступным путем.

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 помимо для достижения своих преступных целей используют не только IT-навыки, программирование, (де)шифрование, социальную инженерию, но и имеющиеся лазейки законе. Киберпреступность давно перешагнула порог от совершения кибератак в одиночку в режиме ALONE до создания целых организованных преступных группировок. К этому процессу также подключились и те, кто раньше осуществлял все преступные замыслы в офлайн режиме, к примеру наркоторговцы, торговцы оружием и так далее.

Возможности глобальной сети Интернет, в том числе и Darknet поражают. В Darknet можно не только приобрести наркотики, конфиденциальные данные клиентов банков или платежных 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 так далее). Особенно команда крайне важна по киберпреступлениям, связанным с завладением чужими денежными средствами, так как каждый член организованной группы выполняет определенные роли. Одним из важных членов данной группировки является тот, кто помогает сокрыть следы преступления и отмыть денежные средства дабы не попасться в сети правоохранительных органов. Он именуется везде по-разному в европейских странах их называют money mull (денежный мул), у нас – дроп.

Проанализированные отчеты подчеркивают, что вопреки тому, что можно было бы ожидать: за денежным мулом стоят не мелкие преступники, а сложные преступные организации. 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 группировками»[1]. Однако, к сожалению, роль дропов или денежных мулов остается 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 путем, в имущество, имеющее вид правомерно полученного, часто связывают с деятельностью известного чикагского гангстера Аль Капоне. Согласно распространенной версии денежные средства, получаемые от бутлегерства – контрабанды в США алкоголя в период действия так называемого «сухого закона», 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.

На сегодняшний день 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 от 500

[1] John Leyden, 178 Arrested in Pan-European Money Mule Crackdown, THE REGISTER (Nov. 22, 2016, 12:59 PM), http://www.theregister.co.uk/2016/11/22/ european money mule-crackdown (quoting Michle Coninsx).
[2] J.C. Sharman, Power and Discourse in Policy Diffusion: AntiMoney Laundering in Developing States, 52 INT'L STUD. Q. 635 (2008),http://www.jstor.org/stable/pdfl29734254.pdfrefreqid=excelsior:445177bdc354bd9a264da04llb4e7Od8&seq=1#page-scantab-contents.
[3] https://eurasiangroup.org/ru/faq

долларов США найти местоположение преступника практически нереально). К тому же для отмывания денег нужен обязательно человеческий капитал – дропы.

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

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

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

В онлайн режиме дропов находят через социальные сети (Telegram, Instagram, Facebook) путем выкладывания разного рода объявлений (ХОТИТЕ ЗАРАБОТАТЬ ДЕНЬГИ БЫСТРО И БЕЗ УСИЛИЙ! ОПЫТ НЕ НУЖЕН! ТОЛЬКО ЖЕЛАНИЕ ЗАРАБОТАТЬ! и так далее). Хотя уровень написания данных объявлений говорит о низкой грамотности дроповодов. Как отметил в своем исследовании Брук С. Чарльз (Brooke S. Charles) «Тем не менее, их образование, по-видимому, довольно базовое, учитывая плохой язык в их электронных письмах о приеме на работу»[8].

После размещения рекламы и объявлений, с ними связываются потенциальные дропы. Как отметили некоторые ученые «Денежных мулов вербуют с использованием различных подходов, часто обманывая роскошным образом жизни, чтобы заинтересовать потенциальных денежных мулов»[9].

---

[4] https://en.wikipedia.org/wiki/Money_mule#:~:text=A%20money%20mule%2C%20sometimes%20called,part%20of%20the%20money%20transferred.

[5] Manny Aston, Stephen McCombie, Ben Reardon, Paul Watters. A Preliminary Profiling of Internet Money Mules: An Australian Perspective. Cybercrime Research Lab, Macquarie University. 978-0-7695-3737-5/09 $25.00 © 2009 IEEEDOI 10.1109/UIC-ATC.2009.63

[6] Rainer Hulsse, The Money Mule: Its Discursive Construction and the Implications, 50 Vanderbilt Law Review 1007 (2021). Available at: https://scholarship.law.vanderbilt.edu/vjtl/vol50/iss4/5

[7] William Vicek, Securitizing Money to Counter Terrorist Finance: Some Unintended Consequences for Developing Economies, 16 INT'L STUD. PERSP. 406, 414-16 (2015).P. 415.

[8] Brooke S. Charles, The Most Common Schemes for Targeting the Unknowing Money Mule, SECURITY INTELLIGENCE (Sep. 16, 2014), https://securityintelligence.com/the-most-common-schemes-for-targeting-theunknowing-money-mule/ (noting that the recruitment emails have poor grammar).

[9] Mohd Irwan Abdul Rani, Sharifah Nazatul Faiza Syed Mustapha Nazri, Salwa Zolkaflil. A systematic literature review of money mule: its roles, recruitment and awareness. Journal of Financial Crime. ISSN: 1359-0790. Article publication date: 5 January 2023

Стоит отметить, что существует несколько видов дропов. ФБР делит «денежных мулов» на три категории в зависимости от их целей и степени вовлеченности: неосведомленные денежные мулы; сознательные денежные мулы; соучастники денежных мулов[10].

Первая категория дропов – не знают, что с помощью них совершается сокрытие следов преступления. Так, по уголовному делу №1-1003-2204/773[11], граждане Ю. и Э., по предварительному сговору 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 платежные карты в последующем использовались для отмывания денег. За каждую платежную карту дроповоды получали 20 долларов США.

Вторая категория дропов, они сами связываются с дроповодами и продают свои платежные карты или номера SIM-карт дроповодам за определенную 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, что оформить платежную карту определенного банка, и через банкомат подключить SMS-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 20.000 до 3 миллионов сум в зависимости от количества, типа платежной карты (VISA, HUMO, UzCard) и банка, в котором открыт банковский счет). Следует отметить, что в данном случае, даже при выявлении дропа выйти на дроповода практически нереально, так как не было физического контакта, и даже аккаунт открывается на купленные в специальных платформах виртуальные номера. Кроме того, даже телефонный номер, который использовался для привязки карты тоже покупается в данных социальных сетях, и деньги, переведенные на счет дропа, также является картой другого дропа.

Хотя Отчет шведских правоохранительных органов[12] утверждают, что становится проблемой найти достаточно наивных людей, согласных стать дропами, однако, как показывает анализ изучения уголовных дел, в каждом случае совершения вишинга, преступниками использовались карты дропов[13].

Возникает вопрос зачем нужны карты дропов? Они играют ключевую роль для того, чтобы истинные преступники остались в тени. Сначала они осуществляют киберпреступление, к примеру фишинг или вишинг, после чего похищенные денежные средства направляются на счет карт-дропов. На карте дропов деньги не остаются 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

[10] https://sanctionscanner.com/knowledge-base/money-mules-248
[11] https://public.sud.uz/report/CRIMINAL
[12] Melani, Informationssicherung. Lage in der Schweiz und International. Halbjahresbericht 2016/1 (JANUAR-JUNI) 41 (2016), https://www.melani.admin.ch/melani/...Ihalbjahresbericht-2016-1.html
[13] Анализ уголовных дел, находящихся в производстве ОБПСИТ города Ташкента. 2024.

выходят на дропов, которые отвечают, что до этого продали карты за определенную сумм денег.

Третья категория дропов – те, которые в курсе того, что благодаря ним отмываются деньги, добытые преступным путем. Но, несмотря на это, они за каждую транзакцию и перевод через его карту получают вознаграждение. Так, по уголовному делу № 1–1007–2201/253 гражданка Н. в мессенджере «Telegram», вступив в преступный сговор с неизвестным лицом с ник-неймом «Mercedes», обговорив заведомо преступный план хищения денежных средств с банковских пластиковых карт граждан, под условием получения 3 процента от краденной суммы Н. предоставила данному лицу доступ к своим банковским пластиковым картам для того, чтобы краденные деньги переводились на её банковские пластиковые карты как на «транзитные» с последующим переводом краденных денежных средств на кошельки платёжного сервиса «QIWI». В данном случае, она была привлечена к уголовной ответственности по статье 243 УК.

Однако, первую и вторую категорию дропов невозможно привлечь к уголовной ответственности в связи с тем, что в нашем законодательстве не предусмотрена уголовная ответственность за продажу и передачу третьему лицу банковской карты, что является главным инструментом для отмывания денег. А привлечь как соучастник по статье 243 УК возможно только после допроса дроповода, который и должен сказать знал дроп об источнике денег, поступавших на его счет или нет, а учитывая сложную схему по вербовке дропа, изобличить дропа очень сложно. Во-первых, понимание того, что денежный мул является невинной жертвой, в значительной степени исключает применение к нему жестких мер. Как было отмечено в отчетах швейцарского ПФР, в которых описывается, как большинству денежных мулов сходит с рук отсутствие штрафов или только небольшие штрафные санкции из-за трудности доказать, что мул осведомлен о преступлении[14].

Дропов в офлайн режиме ищут, как правило среди алкоголиков, бомжей, в студенческих общежитиях и многолюдных местах, где за определенную сумму денег, их просят оформить в ближайшем банке платежную карту или номер SIM-карты, чтобы сразу также пройти онлайн идентификацию в мобильном приложении для последующего осуществления транзакции. В проведенном исследовании в Малайзии было установлено, что синдикаты обычно получают счета денежных мулов (также известные как суррогатные счета) путем обмана тех, кто нуждается в дополнительном доходе и имеет низкий уровень финансовой грамотности[15].

Следует отметить, что не только банковская карта, но номер SIM-карты также является основным предметом сделок между дропами и дроповодами, так как для осуществления регистрации в мобильных приложениях, осуществления транзакции необходима привязка банковской платежной карты к номеру SIM-карты. Однако, схема приобретения SIM-карт немного отличается от получения банковских карт, так как дроповодам в данном случае нужны физические SIM-карты, которые он должен

[14] MROS, Annual Report by the Money Laundering Reporting Office Switzerland MROS 2014, FEDERAL OFFICE OF POLICE 41 (2015), supra note 23, at 49.

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

получить от дропа. В данном случае дроповодов просят оформить на себя номера SIM-карт, желательно несколько штук (в РФ, к примеру правоохранительными органами было изъято 1608 карт у одного дропа[16]) и оставить физические SIM-карты в определенном месте и скинуть локацию, чтобы избежать визуального контакта с дроповодом (аналогичная схема существует и для закладчиков наркотических средств). После выполнения инструкции дропу скидываются денежные средства на указанную им карту.

Номера SIM-карт используются не только для привязки банковской карты, но и для осуществления полноценной транзакции посредством услуги «Мобильный платеж» (фактически сама выполняет роль платежной карты), похищенные денежные средства перенаправляются на другие телефонные номера дропов, а потом через электронные кошелки или крипто биржу, к примеру Binance осуществляются P2P переводы для покупки крипто-активов через обменщиков и, направляя деньги на горячий кошелек самой платформы (Hot Binance) переводятся на другие крипто-кошельки.

Однако, несмотря на то, что номера SIM-карт выступают в качестве орудия по «отмыванию» доходов, добытых преступным путем, являясь необходимым условием для привязки банковской платежной карты и использования Интернет-банкинга, в отношении мобильных операторов, в том числе банковских учреждений, а также лиц, продавших данные номера SIM-карт, не применяется никакая ответственность.

Согласно проведенному опросу среди следователей и дознавателей, 100% респондентов ответили за необходимость введения административной и уголовной ответственности за передачу третьим лица банковской платежной карты и номеров SIM-карт. Указывая, что причиной увеличения количества дропов является отсутствие ответственности за эти деяния, а 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 проведен онлайн-опрос среди более чем 3000 человек в возрасте от 16 до 25 лет, который показал, что к около 10% предлагали стать дропами (как через социальные сети Snapchat и Instagram, так и в офлайн режиме (сверстники в школе, знакомые, друзья). Менее 1% процента признались, что на самом деле были денежным мулом, а некоторые и вовсе считали приемлемым передать свои карты для пользования третьими лицами[19].

Наказания за добровольное предоставление средств платежа мошенникам существуют и весьма суровые. Скажем, в Китае наказание может быть пожизненным (у нас (имеется ввиду в РФ) тоже, в случаях, если дроп замешан в переводе средств, направленных на финансирование терроризма). В Европе – до 10 лет заключения[20].

[16] https://daily.hse.ru/post/1340
[17] Онлайн опрос, проведенный среди сотрудников Управления по борьбе с преступлениями в сфере информационных технологий. 2024.
[18] https://www.ema.com.ua/citizens/cyber-safety-school/do-not-become-a-drop-free-cheese-is-only-in-a-mousetrap/
[19] Luuk Bekkers,Ynze Van Houten,Remco Spithoven &Eric Rutger Leukfeldt/ Money Mules and Cybercrime Involvement Mechanisms: Exploring the Experiences and Perceptions of Young People in the Netherlands.Pages 1368-1385. Published online: 30 Mar 2023
[20] https://nbj.ru/fingramotnost/ekspert-maksim-syemov-vvedenie-ugolovnogo-/62840/ От перемены названий сроки не меняются

Статья 222 УК Республики Беларусь предусматривает уголовную ответственность за незаконный оборот средств платежа и (или) инструментов «… совершенное из корыстных побуждений незаконное распространение реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным кошелькам» вплоть до 10 лет лишения свободы, административной ответственности не предусмотрено.

Статья 191 УК КНР[21] предусматривает уголовную ответственность за содействие в переводе денежных средств путем перечисления на счет или путем использования иных способов расчета; содействие в переводе денежных средств заграницу; утаивание и сокрытие иными способами источников и характера доходов, полученных преступным путем, квалифицируя данные деяние как отягчающее обстоятельство (наказывается до 10 лет лишения свободы и штрафом в размере от 5% до 20% «отмытых денег».

Согласно УК Франции[22] статья 324-1 «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 375 000 евро».

Согласно статье 261 УК ФРГ[23] «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 трех месяцев до пяти лет. Любое лицо, в случаях, предусмотренных подразделами (1) или (2) выше, **по грубой небрежности не осведомленное** 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 переведенные через его карту денежные средства были преступными доходами, не освобождает от уголовной ответственности.

Отсутствие в национальной законодательстве ответственности за передачу платежной карты или номера SIM-карты преступникам и за оказание им других услуг, приводит к соблазну заработать «легкие» деньги за продажу платежной карты или номера SIM-карты, что и приводит к тому, что злоумышленники остаются

[21] http://ru.china-embassy.gov.cn/rus/zfhz/zgflyd/201601/t20160111_3149373.htm
[22] https://www.equalrightstrust.org/ertdocumentbank/french_penal_code_33.pdf
[23]https://www.uni-potsdam.de/fileadmin/projects/ls-hellmann/Forschungsstelle_Russisches_Recht/Neuauflage_der_kommentierten_StGB-%C3%9Cbersetzung_von_Pavel_Golovnenkov.pdf

безнаказанными, а денежные средства жертв утекает на зарубежные счета и не удается обеспечить возмещение материального ущерба.

Основной лазейкой в законодательстве, которое и приводит к массовой вербовке дропов, является отсутствие ответственности. А где не запрещено, там разрешено. Поэтому для предотвращения ухудшения криминогенной ситуации целесообразно внести изменения в законодательство, предусматривающее уголовную ответственность за его совершение. 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 об административной ответственности Республики Узбекистан статьей 179^6 и изложить в следующей редакции:

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

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

влечет наложение штрафа от пятидесяти до ста базовых расчетных величин или административный арест до пятнадцати суток.

То же правонарушение, повлекшее причинение значительного ущерба,

влечет административный арест до пятнадцати суток с наложением штрафа от ста до ста пятидесяти базовых расчетных величин.

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

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

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

наказываются штрафом от ста пятидесяти до трехсот базовых расчетных величин или исправительными работами от двух до трех лет либо лишением свободы до трех лет.

Те же действия, совершенные:

а) по предварительному сговору группой лиц;

б) совершенные повторно или опасным рецидивистом;

в) повлекшие причинение крупного ущерба;

наказываются ограничением свободы от трех до пяти лет или лишением свободы на срок от трех до десяти лет со штрафом в размере от трехсот до пятисот базовых расчетных величин.

Те же действия, совершенные:

а) организованной группой или в ее интересах;

б) повлекшие 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 платежной 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 SIM-карт.

References:

1. John Leyden, 178 Arrested in Pan-European Money Mule Crackdown, THE REGISTER (Nov. 22, 2016, 12:59 PM), http://www.theregister.co.uk/2016/11/22/ european money mule-crackdown (quoting Michle Coninsx).
2. J.C. Sharman, Power and Discourse in Policy Diffusion: AntiMoney Laundering in Developing States, 52 INT'L STUD. Q. 635 (2008),http://www.jstor.org/stable/pdfl29734254.pdfrefreqid=excelsior:445177bdc354bd9a264 da04llb4e7Od8&seq=1#page-scantab-contents.
3. Manny Aston, Stephen McCombie, Ben Reardon, Paul Watters. A Preliminary Profiling of Internet Money Mules: An Australian Perspective. Cybercrime Research Lab, Macquarie University. 978-0-7695-3737-5/09 $25.00 © 2009 IEEEDOI 10.1109/UIC-ATC.2009.63
4. Rainer Hulsse, The Money Mule: Its Discursive Construction and the Implications, 50 Vanderbilt Law Review 1007 (2021). Available at: https://scholarship.law.vanderbilt.edu/vjtl/vol50/iss4/5
5. William Vicek, Securitizing Money to Counter Terrorist Finance: Some Unintended Consequences for Developing Economies, 16 INT'L STUD. PERSP. 406, 414-16 (2015). P. 415.
6. Brooke S. Charles, The Most Common Schemes for Targeting the Unknowing Money Mule, SECURITY INTELLIGENCE (Sep. 16, 2014), https://securityintelligence.com/the-most-common-schemes-for-targeting-theunknowing-money-mule/ (noting that the recruitment emails have poor grammar).
7. Mohd Irwan Abdul Rani, Sharifah Nazatul Faiza Syed Mustapha Nazri, Salwa Zolkaflil. A systematic literature review of money mule: its roles, recruitment and awareness. Journal of Financial Crime. ISSN: 1359-0790. Article publication date: 5 January 2023
8. Melani, Informationssicherung. Lage in der Schweiz und International. Halbjahresbericht 2016/1 (JANUAR-JUNI) 41 (2016), https://www.melani.admin.ch/melani/...Ihalbjahresbericht-2016-1.html
9. Ilyas, I. Y., Ridzuan, A. R., Mohideen, R. S. and Bakar, M. H. (2022). Level of Awareness and Understanding towards Money Mule Among Malaysian Citizens. Journal of Accounting and Finance in Emerging Economies, 8 (4), 481-488

10. Luuk Bekkers,Ynze Van Houten,Remco Spithoven &Eric Rutger Leukfeldt/ Money Mules and Cybercrime Involvement Mechanisms: Exploring the Experiences and Perceptions of Young People in the Netherlands.Pages 1368-1385. Published online: 30 Mar 2023
11. Шестернева Е. Банки смогут блокировать сомнительные платежи // Административное право. – 2018. – №3. – С. 29-32.