УДК 343
DOI https://doi.org/10.24144/2788-6018.2022.05.61

СПОСОБИ ЛЕГАЛІЗАЦІЇ (ВІДМИВАННЯ) МАЙНА, ОДЕРЖАНОГО ЗЛОЧИННИМ ШЛЯХОМ У КІБЕРПРОСТОРІ

Думчиков М.О.,
кандидат юридичних наук, старший викладач кафедри кримінально – правових дисциплін та судочинства ННІ права Сумського державного Університету
ORCID: https://orcid.org/ 0000-0002-4244-2419

Думчиков М.О. Способи легалізації (відмивання) майна, одержаного злочинним шляхом у кіберпросторі.

Поява та розвиток нових фінансових та інформаційних технологій, інтеграція національних економічних систем у світову економіку, розширення господарських зв'язків як на рівні окремої держави, так і на наднаціональному рівні, суттєво полегшують та навіть забезпечують комунікацію злочинців не лише на території окремої країни, але і за її межами. Безперечно, технічні нововведення змінюють галузь фінансових послуг, пропонуючи абсолютно нові продукти, що спрямовано на полегшення доступу до них, проте виникають нові загрози та вразливості для фінансового сектору, такі як кібератаки (шахрайство в Інтернеті) або маніпуляції з обліковим записом.

Актуальність теми дослідження визначається значним обсягом кримінальних інвестицій, що проникають у легальну економіку, скоєнням нових кримінальних правопорушень, використання нових способів вчинення кримінальних правопорушень у кіберпрострі, залучення до злочинної діяльності дедалі більшої кількості осіб, корумпуванням державних чиновників, у тому числі й тих, які покликані боротися зі злочинністю. Відмивання доходів завдає шкоди економічній безпеці фінансової стабільності України. Міжнародний характер цього виду кримінальних правопорушень ускладнює розкриття та розслідування злочинів, тим самим створює «фінансовий ґрунт» злочинним групам (організаціям) для здійснення протиправної, у тому числі й терористичної діяльності.

Усі зусилля, які спрямовані на боротьбу з легалізацією доходів, здобутих злочинним шляхом у кіберпросторі без створення ефективної системи протидії з цим явищем не дають позитивних результатів. Тому протидія легалізації доходів, одержаних злочинним шляхом, вимагає вивчення походження та способів поширення цього суспільно-небезпечного явища, а також належного правового забезпечення, відповідно до міжнародних стандартів.

Ключові слова: легалізація злочинних доходів, кіберлегалізація, кіберзлочин, кримінальні правопорушення у кіберпросторі, легалізація за допомогою віртуальних активів.

Dumchikov M.O. Methods of legalization (laundering) of property obtained by criminal means in cyberspace.

The emergence and development of new financial and information technologies, the integration of national economic systems into the world economy, the expansion of economic ties both at the level of a separate state and at the supranational level significantly facilitate and even ensure the communication of criminals not only on the territory of a separate country, but also its limits. Technical innovations are undoubtedly changing the financial services industry, offering entirely new products aimed at making them easier to access, but new threats and vulnerabilities are emerging for the financial sector, such as cyber-attacks (internet fraud) or account manipulation.

The relevance of the research topic is determined by the significant amount of criminal investments penetrating the legal economy, the commission of new criminal offenses, the use of new ways of committing criminal offenses in cyberspace, the involvement of an increasing number of people in criminal activities, the corruption of state officials, including those called fight crime. Money laundering harms the economic security and financial stability of Ukraine. The international nature of this type of criminal offenses complicates the detection and investigation of crimes, thereby creating a «financial basis» for criminal groups (organizations) to carry out illegal, including terrorist, activities.

All efforts aimed at combating the legalization of proceeds of crime in cyberspace without creating an effective system to combat this phenomenon do not yield positive results. Therefore, combating the legalization of proceeds obtained through crime requires the study of the origin and ways of spreading this socially dangerous phenomenon, as well as proper legal protection, in accordance with international standards.

Key words: legalization of criminal proceeds, cyberlegalization, cybercrime, criminal offenses in cyberspace, legalization using virtual assets.

Постановка проблеми. Сьогодні кримінальні правопорушення в кіберпросторі, тобто які вчиняються сфері комп'ютерної інформації та вчинені за допомогою комп'ютера є одними з найдинамічниших видів суспільно небезпечних посягань. Перш за все це зумовлено прискореним розвитком технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування електронно обчислювальних машин. Також неможна ігнорувати наслідки поширення пандемії COVID-19, яка фактично змусила людей до самоізоляції в умовах карантинних обмежень, і як наслідок стрімке поширення використання електронно обчислювальних машин та інших комп'ютерних гаджетів. Все це зумовило появу нових видів кримінальних правопорушень у кіберпросторі. Одним з таких кримінальних правопорушень хочемо визначити кримінальне правопорушення регламентоване 209 статтею Кримінального кодексу України легалізація майна, одержаного злочинним шляхом.

Стан опрацювання цієї проблематики. Різні аспекти питання легалізації майна одержаного злочинним шляхом у кіберпросторі не втрачають актуальності протягом останніх років та були предметом дослідження таких науковців як: О.М. Резнік, О.С. Бондаренко, М.С. Уткіна, А. Хабіб, С.Д. Грінко, В.В. Коваленко.

Метою статті є: визначення та характеристика нових способів легалізації майна отриманого злочинним шляхом у кіберпросторі. Визначити основні кримінальні правопорушення вчинені у кіберпросторі, які виступають як предикатне діяння при вчинені кримінального правопорушення передбаченого статтею 209 Кримінального кодексу України.

Виклад основного матеріалу. Найбільш поширеними інструментами які використовують кіберзлочинів для легалізації злочинних доходів є [1].

- використання рахунків, відкритих за втраченими або підробленими документами;
- відкриття рахунку, в т. ч. карткових на ім'я малозабезпечених громадян та підприємств з ознаками фіктивності;
- використання міжнародних платіжних систем (електронні платежі);
- проведення ланцюгових фінансових потоків через декілька банківських рахунків за допомогою дистанційного доступу;
- електронні кошти та криптовалюти;
- використання підставних осіб.

Найбільш поширеними способами відмивання злочинних доходів, які використовують в своїй діяльності кіберзлочинці, є:

- відмивання злочинних доходів через електронні платіжні системи та онлайн банкінг
- відмивання злочинних доходів через шахрайські дії у кібер просторі
- відмивання злочинних доходів через онлайн казино
- відмивання злочинних доходів шляхом переведення готівкових коштів в електронні гроші та подальше придбання товарів

Найпопулярнішими і поширеними формами відмивання грошей в кіберпросторі є так званий «ланцюжок фінансових операцій» через кілька банківських рахунків з віддаленим доступом, використання готівки на останньому етапі ланцюга фінансових операцій, купівля електронних грошей і використання платежів системи через електронні гаманці з подальшою трансформацією незаконних доходів у товари, через онлайн-покупку тощо.

Варто зауважити, що кіберзлочинці дуже часто використовують у своїй діяльності можливості платіжних систем та так званих «цифрових грошей». Для відмивання злочинних грошових коштів вони використовують як внутрішньодержавні так і міжнародні платіжні системи, серед яких найбільшу популярність серед злочинців мають WebMoney, Skrill, Transferwise, LibertyReserve, wires та інші.

Також злочинці активно використовують такі способи виведення злочинних коштів із систем електронних грошей як: банківський переказ, оплата готівкою через системи грошових переказів Western Union та подібні системи, оплата готівкою через спеціалізований пункт обміну електронної валюти.

Існує велика кількість методів введення/випуску електронної валюти, що робить їх легкодоступними та зручними для користувачів, а також спрощує та просуває можливості їх використання для незаконних грошових операцій.

Напевно найпривабливішою галуззю економіки для відмивання злочинних доходів з використанням різноманітних фінансових послуг та інструментів виступає банківський сектор.

У банківській сфері України найбільша питома вага злочинів пов'язана з кредитуванням, незаконним зняттям грошових коштів з рахунків, привласненням депозитів, маніпуляції з первинними документами, що призводить до викривлення фінансової звітності. Слід зазначити, що значна кількість дрібних банків були збанкрутовані самими засновниками. Схема була стандартна: після реєстрації банку залучено нових клієнтів, які переходили на розрахунково-касове обслуговування в установах банку або клали в банк гроші на депозит, активно залучали ресурси з міжбанківського кредитування. Після акумуляції в банку достатньої суми засновникам банку видавалися дуже великі кредити, які в сукупності робили банк неплатоспроможним [1].

Хочемо звернути, увагу на те, що сьогодні сучасні банківські технології дозволяють підвищити анонімність незаконних транзакцій. Адап-

тація банківського сектору до сучасних онлайн викликів, забезпечила стрімкий та динамічний розвиток P2P-платежів, які знаходяться на передовій електронно фінансового бізнесу. Одночасно з розвитком системи P2P-платежів, розширюються і способи ведення злочинних операцій з ними. Транзакції P2P (від людини до людини) набули популярності в 2020 році завдяки швидкості проведення транзакцій, анонімності, та невисоким комісіям за транзакцію [2].

Одним з найпоширеніших способів отримання злочинних доходів у P2P-діяльності виступає фішинг. Фішинг – одна з найпоширеніших форм шахрайства з платіжними картками в Інтернеті, спрямована на отримання конфіденційної інформації про дані картки та інших персональних даних від жертви.

Фішингові веб-сайти є сайтами клонами оригінальних веб-сайтів, які ззовні зовсім не відрізняються від оригіналу, проте мають деякі незначні і на перший погляд непомітні назви у домені веб-сайту. Це можуть бути «сайти клони» різноманітних банківських установ, платіжних систем, онлайн магазинів, де потрібно ввести дані своєї банківської картки. Після отримання даних банківської карти жертви, зловмисники можуть використати їх на свій розсуд, такий процес називають кардингом.

Найпоширенішим способом легалізації злочинних доходів шляхом кардингу є купівля товарів на різноманітних вітчизняних сайтах онлайн комерції за викрадені кошти. Суть схеми полягає у тому, що особа купуючи товар на оналайн маркет плейсі, переводить продавцю товару суму значно більшу ніж коштує товар. Наступним етапом зазначеної схеми буде повідомлення продавця товару про помилкове перерахування коштів, через що продавець перераховує різницю зловмиснику на карту. Таким чином зловмисник має «чисті» гроші, а продавцю товару через декілька днів, банк блокує рахунок за отримання «брудних коштів», а сама жертва стає в очах правоохоронних органів зловмисником.

З огляду на останні світові події, тенденцією 2020 року, пов'язаною з пандемією коронавірусу COVID-19, стало відмивання грошей. Все більше державних установ, юридичних та фізичних осіб переходять на онлайн-системи, щоб запропонувати дистанційну роботу. Люди, які перебувають на карантині (або підпадають під інші обмежувальні заходи), також все частіше звертаються до різноманітних онлайн-платформ, щоб залишатися соціальними. Представники кримінального світу використовують ситуацію з COVID-19 для легалізації незаконних заробітків, формуючи різноманітні схеми.

Економічна криза, викликана COVID-19, призвела до збільшення шахрайських інвестиційних схем, включаючи рекламні кампанії, які оманливо стверджують, що продукти чи послуги певних державних компаній можуть запобігти, виявити або вилікувати COVID-19. Так, акції мікрокапіталізації зазвичай випускаються дуже малими компаніями і можуть бути особливо вразливими до схем інвестиційного шахрайства, оскільки вони дуже дешеві і про них дуже мало публічної інформації. Все це призводить до поширення недостовірної інформації про компанії. Тому останнім часом зросла кількість соціально-інженерних атак, особливо фішингових листів і мобільних повідомлень, надісланих як спам. Ці атаки використовують посилання на оманливі веб-сайти або шкідливі вкладення для отримання особистої платіжної інформації [3].

Злочинці також знаходять способи відмивання грошей у таких сферах, як краудфандинг. Зокрема, краудфандингові платформи для акціонерного капіталу можна використовувати принаймні двома способами для сприяння відмиванню грошей [4].

По-перше, продавець незаконних товарів, таких як наркотики або незареєстрована вогнепальна зброя, може створити фальшиву компанію та продавати свої цінні папери на будь-якій фінансовій платформі. В результаті покупці можуть «легально» придбати через платформу акції неіснуючої компанії. Таким чином, дистриб'ютори отримують кошти в електронному вигляді, а не готівкою, і можуть об'єднати декілька платежів в один грошовий потік [5].

Стрімкий розвиток азартних ігор в мережі Інтернет, зумовлений перш за все технологіями, які динамічно розвиваються і я результат полегшують до ресурсів онлайн простору. Варто зазначити, що така діяльність характеризується транскордонною ознакою, адже сервери для розміщення онлайн казино можуть перебувати в будь – якій точці світу включаючи офшорні юрисдикції. Така ситуація призводить до юрисдикційних та законодавчих прогалин.

В умовах швидкого зростання ринку азартних ігор в онлайн просторі велика кількість країн почали їх легалізувати, однак з дуже суровими правилами щодо їх діяльності. Однак злочинці пристосовуються до нових правил гри та використовують онлайн азартні ігри для відмивання злочинних доходів, шляхом конвертації готівкових коштів в «ігрову валюту казино», виведення її на електронні гаманці і подальше придбання товарів.

Комітет Ради Європи з оцінки заходів боротьби з відмиванням грошей у 2020 році навели класифікацію держав за регулюючою ознакою грального онлайн бізнесу [6, с. 21]:

1. Держави де онлайн азартні ігри врегульовані на законодавчому рівні. Власники онлайн казино здійснюючи діяльність на території таких держав може просувати свої послуги в інтернет мережі.

2. Держави в яких онлайн азартний бізнес не заборонено але і не врегульовано. Найчастіше

саме такі країни відносяться до списку найбільш уразливих для відмивання злочинних доходів.

3. Держави в яких онлайн азартний бізнес повністю заборонено. Доходи від такої діяльності в таких країнах є повністю протизаконними, як і сама діяльність такого бізнесу.

Зазначмо, що Україна входить до першої групи країн, де організації і діяльність азартних ігор є законною відповідно до Закону України «Про державне регулювання діяльності з організації та проведення азартних ігор» від 13 серпня 2020 року. Законом визначено основні види азартних ігор які дозволені в Україні, а саме (Bill № 768-IX, 2020): організація та проведення азартних ігор в гральних закладах казино,

- казино в мережі Інтернет,
- букмекерської діяльності в букмекерських пунктах та в мережі Інтернет,
- ігор в залах гральних автоматів, азартних ігор в покер в мережі Інтернет.

Перелічені види діяльності у сфері організації та проведення азартних ігор на території України можуть проводитися виключно за наявності у суб'єкта господарювання відповідних ліцензій із використанням сертифікованого та підключеного до Державної системи онлайн-моніторингу грального обладнання та онлайн-систем організаторів азартних ігор [7]. Ще одним способом відмивання злочинних доходів можна визначити переведення готівкових злочинних коштів в систему електронних грошей типу skrill, nettler, advego, wires та інші, та подальше придбання через такі сервіси товарів в Інтернеті. Суть даної схеми пропонуємо розкрити в декількох етапах її реалізації.

На першому етапі зловмисники переводять готівкові кошти отриманих від злочинної діяльності в електронні онлайн платіжні системи. Такими системами можуть виступати PayPal, Skrill, Neteller, Payoneer, Perfect Money, ChronoPay, WebMoney, Яндекс.Деньги, Qiwi, RBK Money, PayCash, ЮMoney, ГлобалМані, EasyPay, LiqPay, iPay.ua, Простір. Для більш довірливого стану створюються декілька акаунтів у зазначених платіжних системах на так званих «дропів» – (від англійського слова drop скидати) особа на особисті данні якої реєструються акаунти платіжної системи для подальшої злочинної діяльності, але при цьому дана особа не знає про таку діяльність. Створення великої кількості акаунтів у платіжній системи, дасть змогу розкинути злочинні готівкові грошові кошти на кожен створений акаунт в платіжній системі невеликі суми, тим самим отримати менше уваги з бору безпекового сектору платіжної системи.

На другому етапі зловмисники реєструють фіктивний суб'єкт підприємницької діяльності як той, що сплачує єдиний соціальний внесок на 3 групі платника податків.

На третьому етапі створюється веб – сайт з продажу онлайн товарів чи надання онлайн послуг, та підключається мерчант системи зазначених платіжних систем для оплати товарів та послуг. Також зловмисники можуть скористатися вже готовими маркет плейсами які використовують зазначені вище платіжні системи. На завершальному етапі зловмисники купують товари чи послуги самі в себе і отримають «чисті» легальні грошові кошти.

Хочемо наголосити, що динамічний розвиток інформаційних Інтерент – технологій став певним підґрунтям переплетення національних економік усіх держав світу, все це активно сприяє розвитку легалізації злочинних доходів. Ба більше злочинці стрімко розвивають методи відмивання злочинних доходів, знаходячи та використовуючи лазівки в системах переміщення грошей з використанням кіберпростору.

Висновки. Розвиток інформаційних технологій та диджиталізація суспільства в цілому та економіки держави зокрема, дала поштовх до пошуку зловмисниками нових схем легалізації злочинних доходів. Зловмисники у своїй діяльності щодо легалізації злочинних доходів здатні використовувати новітні технологічні інструменти, такі як Інтернет банкінг, криптовалюти, електронні платіжні системи. Такий широкий спектр інструментів дозволяє переміщувати злочинні кошти як в середні країни так і за кордон з надзвичайною швидкістю. Створення анонімних транзакцій ускладнює фінансовий моніторинг за такими операціями, як підсумок спостерігається динамічне зростання кримінальної активності у сфері відмивання доходів отриманих злочинним шляхом.

Викриття схем, які пов'язані з легалізацією злочинних доходів, вважаємо основним завданням всіх суб'єктів системи запобігання та протидії легалізації доходів, одержаних злочинним, а враховуючи транскордонний характер такого діяння, особливої уваги набуває міжнародна співпраця у сфері викриття та припинення цього злочинного діяння.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Типологія Держфінмоніторингу. Державна служба фінансового моніторингу. Офіційний сайт. ULR: https://fiu.gov.ua/pages/dijalnist/tipologi/tipologi-derzhfinmonitoringu (дата звернення 14 листопада 2022 р.).
2. Dumchikov, M., Reznik, O. and Bondarenko, O. (2022), «Peculiarities of countering legalization of criminal income with the help of virtual assets: legislative regulation and practical implementation», Journal of Money Laundering Control, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JMLC-12-2021-0135.

3. Rise in time and financier terroirism, affected by COVID-19, and other times in the political arena, FATF. URL: https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT_rus.pdf (дата звернення 14 листопада 2022 р.).
4. Habib, A. ACFCS Special Contributor Report: Crowdfunding-An unorthodox way of Money Laundering? Definitely maybe. ACFCS. URL: https://www.acfcs.org/acfcs-special-contributorreport-crowdfunding-an-unorthodox-way-of-money-laundering-definitelymaybe/ (дата звернення 14 листопада 2022 р.).
5. Simpson, A., Seagrave, S. Lords of the Rim: the invisible empire of the overseas. Crowdfunding: A Coverfor Mone Laundering? URL: https://www.caseware.com/alessa/blog/crowdfunding-cover-money-laundering/ (дата звернення 14 листопада 2022 р.).
6. Choi, S. Illegal Gambling and Its Operation via the Darknet and Bitsoin: An Application of Routine Activity Theory. International Journal of Cybersecurity Intelligence & Cybercrime. Vol. 3. №. 1. pp. 3–23.
7. Азартні ігри в Україні. Що варто знати громадянам. Офіційний сайт Міністерства Юстиції України. URL: https://minjust.gov.ua/m/azartni-igri-v-ukraini-scho-varto-znati-gromadyanam.