

DOI <https://doi.org/10.51647/kelm.2020.3.4.25>

CHARAKTERYSTYKA WYKROCZEŃ KARNYCH POPEŁNIANYCH W GOSPODARCE CYFROWEJ

Oleksandr Markushyn

student Uniwersytetu Współczesnej Wiedzy (Kijów, Ukraina)

ORCID ID: 0000-0003-2339-1590

e-mail: oleksandrmarkushyn@gmail.com

Adnotacja. W artykule scharakteryzowano wykroczenia karne popełniane w sferze cyfryzacji gospodarki. Należy zauważyć, że cyfryzacja gospodarki jest obecnie jednym z najważniejszych obszarów polityki państwa Ukrainy. Proces ten stwarza duże możliwości obywatelom w zakresie usług publicznych, informacji, przyspiesza procesy gospodarcze. Wraz z tym cyfryzacja stwarza również korzystne możliwości dla zorganizowanych grup przestępczych, które przeprowadzają pranie pieniędzy uzyskanego w drodze przestępstwa, oszustwa i inne przestępstwa. Takie bezprawne czyny karne stwarzają poważne zagrożenie dla rozwoju gospodarczego Ukrainy, dlatego warto je rozważyć i określić kierunki zapobiegania popełnieniu takich wykroczeń karnych. Udowodniono, że przestępcze programy wycofania aktywów z Ukrainy w celu wzbogacenia powodują poważne szkody dla sektora gospodarczego. Jednym z obszarów zapobiegania temu jest zastosowanie sztucznej inteligencji, która zapewni dogłębną analizę przepływów finansowych w czasie rzeczywistym i może zapewnić szybkie działanie i szybką identyfikację podejrzanych działań.

Słowa kluczowe: cyfryzacja, przestępczość, gospodarka, przestępczość, wykroczenia karne, środowisko elektroniczne.

CHARACTERISTICS OF CRIMINAL OFFENSES COMMITTED IN THE SPHERE OF THE DIGITAL ECONOMY

Oleksandr Markushyn

winner of the University of Modern Knowledge (Kyiv, Ukraine)

ORCID ID: 0000-0003-2339-1590

e-mail: oleksandrmarkushyn@gmail.com

Abstract. The article describes criminal offenses committed in the field of digitalization of the economy. It is noted that digitalization of the economy is currently one of the most important directions of the state policy of Ukraine. This process creates greater opportunities for citizens to access public services, information, and speeds up economic processes. Along with this, digitalization also creates profitable opportunities for organized criminal groups that carry out money laundering, fraud and other criminal offenses. Such criminally illegal acts pose a serious threat to the economic development of Ukraine, that is why it is expedient to consider them and determine directions for preventing the commission of such criminal offenses. It has been proven that criminal schemes to withdraw assets from Ukraine for the purpose of enrichment cause serious damage to the economic sector. One way to prevent this is through the use of artificial intelligence, which provides real-time in-depth analysis of financial flows and can provide quick action and rapid detection of suspicious activity.

Key words: digitalization, crime, economy, crime, criminal offenses, electronic environment.

ХАРАКТЕРИСТИКА КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ЩО ВЧИНЯЮТЬСЯ У СФЕРІ ЦИФРОВОЇ ЕКОНОМІКИ

Олександр Маркушин

здобувач Університету сучасних знань (Київ, Україна)

ORCID ID: 0000-0003-2339-1590

e-mail: oleksandrmarkushyn@gmail.com

Анотація. У статті охарактеризовано кримінальні правопорушення, які вчиняються у сфері цифровізації економіки. Зазначено, що цифровізація економіки на сьогодні є одним з найважливіших напрямів державної політики України. Цей процес створює більші можливості громадянам до державних послуг, інформації, пришвидшує економічні процеси. Поряд з цим, цифровізація створює й вигідні можливості для організованих злочинних угруповань, які здійснюють відмивання майна, отриманого злочинним шляхом, шахрайства та інших кримінальних правопорушень. Такі кримінально протиправні діяння створюють серйозну загрозу економічному розвитку України, саме тому доцільно розглянути їх та визначити напрями запобігання вчиненню таких кримінальних правопорушень. Доведено, що злочинні схеми щодо виведення активів з України з метою збагачення заподіюють серйозну шкоду економічному сектору. Одним із напрямів запобігання цьому є застосування штучного інтелекту, який надає реальний глибокий аналіз потоків фінансів у реальному часі та може забезпечити швидку дію та стрімке виявлення підозрілих дій.

Ключові слова: цифровізація, злочинність, економіка, злочинність, кримінальні правопорушення, електронне середовище.

Постановка проблеми. Цифровізація економіки на сьогодні є одним з найважливіших напрямів державної політики України. Цей процес створює більші можливості громадянам до державних послуг, інформації, приривидшує економічні процеси. Поряд з цим, цифровізація створює й вигідні можливості для організованих злочинних угруповань, які здійснюють відмивання майна, отриманого злочинним шляхом, шахрайства та інших кримінальних правопорушень. Такі кримінально протиправні діяння створюють серйозну загрозу економічному розвитку України, саме тому доцільно розглянути їх та визначити напрями запобігання вчиненню таких кримінальних правопорушень.

Аналіз останніх досліджень та публікацій. Окремі аспекти злочинності у сфері цифрової економіки та напрямів запобігання розглядалися у фундаментальних працях таких науковців, як: В.М. Бутузов, С.В. Демедюк, В.В. Марков, О.В. Орлов, С.М. Рогозін, В.С. Цимбалюк, та інших.

Проте, незважаючи на суттєві наукові доробки, й дотепер на національному рівні залишаються невирішеними проблеми, пов'язані, зокрема, із розробленням заходів запобігання злочинності у сфері цифрової економіки, аналізу окремих видів кримінальних правопорушень, що вчиняються у цій сфері тощо.

Мета статті – аналіз кримінальних правопорушень, які можуть вчинятися у сфері цифрової економіки та пошук напрямів їх запобігання.

Виклад основного матеріалу. Для початку потрібно зазначити, що найбільш розповсюдженим кримінальним правопорушенням, що вчиняється у сфері цифрової економіки, є відмивання майна, одержаного злочинним шляхом.

Під терміном «відмивання» грошей мають на увазі перетворення незаконно отриманих грошей на легальні. Науковці, що досліджують питання відмивання грошей, пропонують різні визначення цього явища. Так, наприклад на думку Н.М. Мироненко, під «відмиванням» коштів необхідно розуміти інвестування зароблених злочинним способом коштів або їх переказ із метою приховування джерел їх надходжень (Мироненко, 2001: 25–28).

За визначенням В.А. Журавель, спосіб легалізації злочинних доходів являє собою систему різних дій, операцій та прийомів, яка спрямована на підготовку до визнання та приховання, маскуванню її наслідків, а також безпосереднє введення незаконних доходів у легальний сектор (Журавель. Панов, Шепітько, Коновалова, 2008: 322–335).

З іншого боку, Група з розроблення фінансових заходів боротьби з відмиванням грошей (FATF) зазначає, що метою великої кількості кримінально протиправних діянь є отримання прибутку особою чи групою, яка здійснює діяння. Відмивання грошей – це обробка цих злочинних доходів із метою замаскувати їх незаконне походження. Цей процес має вирішальне значення, оскільки він дозволяє злочинцю отримувати ці прибутки, не загрожуючи їх джерелам (Бухтіарова, Відменко, Гавриш, 2020).

На сьогодні в Україні відмивання майна, одержаного злочинним шляхом, досить часто здійснюється з використанням інформаційних технологій, виведенням коштів, активів з нашої держави, зокрема, за допомогою криптовалют. Так, цифровізація економіки призводить до появи нових засобів платежу, які є електронними, та проведення розрахунків за допомогою їх.

На жаль, публічна доступність технологій розрахунків і їх глобальне поширення стало причиною того, що ці технології можуть бути використані незаконним шляхом із метою відмивання грошей через мережу Інтернет. Найбільш популярними та широкоживаними формами легалізації кримінально протиправних доходів Інтернет-шляхом є проведення ланцюга фінансових операцій через кілька банківських рахунків за допомогою віддаленого доступу, використання готівки на останньому етапі ланцюга фінансових операцій, купівля електронних грошей і використання систем платежів через електронні гаманці, конвертація незаконних доходів в товари шляхом їх придбання через Інтернет тощо (Ивашенко, Кужукина, 2018: 113-115).

Злочинці активно використовують у своїх цілях можливості платіжних систем і електронних грошей. Для руху відмитих доходів вони користуються як внутрішньодержавними, так і міжнародними платіжними системами, серед яких WebMoney, LibertyReserve, децентралізована система Bitcoin, віртуальна валюта E-Gold та ін. (Віртуальне майбутнє відмивання грошей, 2020).

Найбільш розповсюдженим сектором економіки, у якому активно використовуються «електронні гроші» та здійснюється відмивання незаконних доходів, є банківська система. Саме за допомогою банків можна безперешкодно переводити конти, здійснювати інші операції з високим рівнем анонімності.

З огляду на це потрібно відмітити, що поширеним способом отримання кримінально протиправних доходів у Р2Р-переказах виступає фішинг – сучасний вид онлайн-шахрайства, за якого злочинці викрадають номери банківських карт, PIN-коди, паролі до онлайн-банкінгу та іншу конфіденційну інформацію. Фішингові сайти є сайтами-підробками, які зовні не відрізняються від «оригіналу». Це може бути «сайт-близнюк» банку, платіжної системи, Інтернет-магазину або будь-якого іншого сервісу, де потрібно вводити дані банківської картки (Bartlett, 2020).

Злочинці знаходять шляхи відмивання доходів і в такій сфері, як краудінвестинг. Зокрема, платформи акціонерного краудфандингу можуть бути використані для полегшення відмивання грошей принаймні двома способами. Так, за першим способом продавець незаконного товару, наприклад наркотиків або незареєстрованої вогнепальної зброї, може створити фальшиву компанію та продати її цінні папери на платформу довільного фінансування. У результаті покуписці можуть «законно» придбати акції неіснуючого підприємства через платформу. Таким чином, дистриб'ютори отримують кошти в електронному вигляді, а не готівкою, а також мають змогу агрегувати кілька платежів в один потік капіталу (Habib, 2020).

Відмітимо, що онлайн-компонент платежів полегшує їхню інтеграцію у фінансову систему. За другим сценарієм дистриб'ютор аналогічно має можливість створити незареєстроване підприємство та продати свої цінні папери через платформу краудінвестингу. Далі, використовуючи Інтернет-псевдонім, той самий дистриб'ютор також інвестує незаконно отримані гроші у власне підприємство, що полегшує переміщення незаконно отриманих доходів через кордон. Це пов'язано насамперед із поширенням транскордонного краудфандингу, який фактично не регулюється на законодавчому рівні (Metsik, 2020).

Як ми вже відмічали, зараз все частіше з'являються фінансові кримінальні правопорушення, які вчинені з використанням криптовалюти. Так, Європолом було проаналізовано її обсяг, у результаті чого визначено, що найбільшу популярність криптовалютні ресурси набувають у кримінальному середовищі. Одним з найпопулярніших методів для відмивання грошей в цій сфері є так зване нашарування. У традиційних фінансах це виглядає як використання «брудних» грошей для купівлі якогось досить дорогого активу. Найчастіше для цих цілей використовують об'єкти нерухомості. Через довгий ланцюжок підставних компаній така нерухомість перепродається суттєву кількість разів, через що встановити реального покупця стає дуже проблематично (Bitcoin і злочинність: як криптовалюти допомагають відмивати гроші, 2018).

Ця схема успішно перенесена на цифрові активи. Спершу на «брудні» гроші купується криптовалюта. Потім, використовуючи спеціалізовані сервіси-міксери, що можна визначити як цифровий аналог пралень Аль Капоне, придбана криптовалюта розділяється на безліч частин, які конвертуються в інші доступні токени. Таким чином, великий криптовалютний потік розбивається на величезну кількість «струмочків», які проходять через сотні і тисячі адрес. Зрозуміло, що визначити реального власника в такому разі більш ніж проблематично (Риски отмивання денег и финансирования терроризма, связанные с COVID-19, и ответные меры в области политики, 2020).

Ще одним досить популярним у зловмисників способом відмивання брудних грошей є ігрова індустрія. Азартні ігри завжди були магнітом для людей, які мають намір перетворювати доходи від злочину у легалізовані гроші. Це галузь, яка характеризується величезними сумами грошей, що рухаються з місця на місце із запаморочливою швидкістю. Сьогодні більше третини ігрової індустрії становить онлайн-ринок. Сума грошових коштів, що надходить через каси цифрових спортивних книг та онлайн-казино, є астрономічними (Риски отмивання денег и финансирования терроризма, связанные с COVID-19, и ответные меры в области политики, 2020).

Криптоказино є окремою галуззю, через яку дуже зручно «відмивати» крадену криптовалюту. На окремий рахунок вноситься певна сума, далі робляться невеликі ставки, після чого гроші виводяться у законний обіг.

Варто відмітити, що через пандемію COVID-19 різко збільшилось відмивання доходів за допомогою криптовалюти. Державні органи переходять на онлайн-роботу, фізичні особи реєструються на багатьох сайтах, оскільки мають більше вільного часу. Представники кримінальних структур, використовуючи цю ситуацію, формують багатоманітні схеми щодо відмивання грошей.

Економічна криза, викликана COVID-19, призвела до збільшення кількості шахрайських схем з інвестиціями, включаючи рекламні кампанії, в яких обманним чином заявляють про те, що продукція або послуги певних акціонерних компаній відкритого типу можуть запобігти, виявити або вилікувати COVID-19. Так, акції з мікрокапіталізацією зазвичай випускаються дуже невеликими компаніями, можуть бути особливо уразливі для шахрайських схем з інвестиціями, оскільки ці акції дуже дешеві, а загальнодоступної інформації про них дуже мало. Все це призводить до поширення недостовірної інформації про компанії. Так, останнім часом різко збільшилася кількість соціо-інженерних атак, особливо фішингових електронних листів і мобільних повідомлень, що розсилаються як спам (Риски отмивання денег и финансирования терроризма, связанные с COVID-19, и ответные меры в области политики, 2020). Досить часто на електронні пошти розсилають посилання на шкідливі сайти з метою отримання особистої платіжної інформації.

Інструмент фішингових сайтів добре прижився і на фоні глобальної пандемії. Зокрема, злочинці використовують у своїх інтересах напружену ситуацію навколо COVID-19 для того, щоб встановлювати шкідливі програми на персональні комп'ютери або мобільні пристрої через фішингові атаки шляхом розсилання листів по електронній пошті. Так, кіберзлочинці видавали себе за представників Всесвітньої організації охорони здоров'я і відправляли електронні листи і мобільні повідомлення з тією метою, щоб люди натиснули на шкідливі посилання або відкрили вкладення, в результаті чого злочинці дізнавалися їхні логін і пароль (Риски отмивання денег и финансирования терроризма, связанные с COVID-19, и ответные меры в области политики, 2020).

Інші приклади включають у себе ситуації, коли злочинці розсилають SMS-повідомлення, видаючи себе за представників органів влади, з тією метою, щоб люди зайшли на фіктивні сайти державних органів влади, тим самим дозволивши шахраям отримати інформацію щодо їхніх особових рахунків та/або відомостей особистого характеру про їхні логіни і паролі (Риски отмивання денег и финансирования терроризма, связанные с COVID-19, и ответные меры в области политики, 2020).

Зважаючи на розвиток нових технологій та появу у зв'язку з цим нових способів приховування незаконних доходів актуальним питанням є боротьба з відмиванням грошей. Конфлікт між різними фінансовими секторами та відмиванням доходів привів до того, що фінансові установи створили технологічно-інтелектуальну зброю. Сьогодні для ефективної боротьби з різними фінансовими кримінальними правопорушеннями починають використовувати складні аналітичні технології, такі як машинне навчання.

Варто відмітити, що останнім часом у правоохоронних органах України побутує думка щодо використання штучного інтелекту при розслідуванні кримінальних правопорушень. Зазначається, що машинне навчання та штучний інтелект є найбільш трансформаційними, допомагаючи виявити та деактивувати до 98% випадків, пов'язаних із незаконними операціями.

Окрім цього, така практика присутня й за кордоном. Так, наприклад, у 2020 р. компанія RegTech MAP FinTech представила своє програмне забезпечення, яке покликано допомогти фінансовим компаніям контролювати та перевіряти транзакції з метою запобігання відмиванню грошей. Це програмне забезпечення дозволяє компаніям щодня або в режимі реального часу контролювати транзакції своїх клієнтів для виявлення підозрілої активності. Воно було розроблено з метою допомогти фірмам виконувати свої нормативні вимоги щодо протидії відмиванню грошей та боротьбі з фінансуванням тероризму (MAP FinTech launches AI-powered solution to boost anti-money laundering compliance, 2020).

Висновки. Отже, запобігання злочинності у сфері цифрової економіки є важливим завданням державної політики на сьогодні. Злочинні схеми щодо виведення активів з України з метою збагачення заповдіюють серйозну шкоду економічному сектору. Одним із напрямів запобігання цьому є застосування штучного інтелекту, який надає реальний глибокий аналіз потоків фінансів у реальному часі та може забезпечити швидку дію та стрімке виявлення підозрілих дій. Штучний інтелект має дві основні переваги для банків, які беруть участь у цій битві: підвищує ефективність розслідування фінансових злочинів та управління ризиками установи.

Список використаних джерел:

1. Бухтіарова А.Г., Відменко Ю.В., Гавриш Ю.С. Сучасні тенденції розширення схем відмивання доходів, отриманих злочинним шляхом. *Гроші, фінанси і кредит*. 2020. № 3(77)-2. С. 58–64. Віртуальне майбутнє відмивання грошей? *Поліграф. Перша спеціалізована компанія з виявлення брехні* URL: <https://hr-security.ua/ua/v%D1%96rtualne-maybutn%D1%94-v%D1%96dmivannya-groshey>
2. Журавель В.А. Панов М.І., Шепітько В.І., Коновалова В.О. Розслідування легалізації (відмивання) доходів, одержаних злочинним шляхом. Настільна книга слідчого: наук.-практ. видання для слідчих і дізнавачів. 2-ге вид., перероб. і доп. К.: Вид. дім «Ін Юре», 2008. С. 322–335.
3. Иващенко А.С. Кужукина Ю.С. Новые технологии платежей и расчетов как способ отмывания денег. *Перспективы науки и общества в условиях инновационного развития: Агентство международных исследований*. 2018. С. 113–115.
4. Мироненко Н.М. Легалізація (відмивання) коштів – різні підходи до поняття: бюлетень з обміну досвідом роботи. *МВС України*. 2001. № 136. С. 25–28.
5. Полякова В.В. Легалізація (відмивання) грошових коштів та іншого майна, здобутих злочинним шляхом (проблеми кримінально-правової кваліфікації). *Наукові записки сучасних вчених: праці 23 міжнар. наук.-практ. конф. (Вінниця, 26 жовтня 2018 р.)*. Вінниця, 2018. С. 34–38.
6. Риски отмывания денег и финансирования терроризма, связанные с COVID-19, и ответные меры в области политики. *ФАТФ*. Франция, 2020. URL: https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT_rus.pdf
7. Bartlett M. How does money laundering work through P2P lending? *Quora*. 2020. URL: <https://www.quora.com/How-does-money-laundering-work-through-P2P-lending>
8. Bitcoin і злочинність: як криптовалюти допомагають відмивати гроші. *Finance.ua*. 2018. URL: <https://news.finance.ua/ua/news/-/432104/bitcoin-i-zlochynnist-yak-kryptovalyuty-dopomagayut-vidmyvaty-groshe>
9. Habib A. ACFCS Special Contributor Report: Crowdfunding-An unorthodox way of Money Laundering? Definitely maybe. *ACFCS*. 2020. URL: <https://www.acfcs.org/acfcs-special-contributor-report-crowdfunding-an-unorthodox-way-of-money-laundering-definitelymaybe/>
10. MAP FinTech launches AI-powered solution to boost anti-money laundering compliance. *FinTechGlobal*. 2020. URL: <https://member.fintech.global/2020/04/03/map-fintech-launches-ai-powered-solution-to-boost-anti-money-laundering-compliance/>
11. Metsik M. Crowdfunding platforms and anti-money laundering activities. *Estateguru blog*. 2020. URL: <https://blog.estateguru.co/crowdfunding-platforms-and-anti-money-laundering-activitiesaml/>

References:

1. Bukhtiarova, A.H., Vidmenko, Yu.V., Havrysh, Yu.S. (2020). Suchasni tendentsii rozshyrennia skhem vidmyvannia dokhodiv, otrymanykh zlochynnym shliakhom [Modern trends in the expansion of schemes for laundering proceeds of crime]. *Hroshi, finansy i kredyt*. № 3(77)-2. pp. 58–64. [in Ukrainian].
2. Virtualne maybutnie vidmyvannia hroshey? [The virtual future of money laundering?]. *Polihraf. Persha spetsializovana kompaniia z vyavleniia brekhni*. URL: <https://hr-security.ua/ua/v%D1%96rtualne-maybutn%D1%94-v%D1%96dmivannya-groshey> [in Ukrainian].
3. Zhuravel, V.A. Panov, M.I., Shepitko, V.I., Konovalova, V.O. Rozsliduvannia lehalizatsii (vidmyvannia) dokhodiv, oderzhanykh zlochynnym shliakhom [Investigating the legalization (laundering) of proceeds of crime]. *Nastilna knyha slidchoho: nauk.-prakt. vydannia dlia slidchych i diznavachiv*. 2-he vyd., pererob. i dop. K.: Vyd. dim «In Yure», 2008. pp. 322–335. [in Ukrainian].
4. Ivashchenko, A.S. Kuzhukina, Yu.S. (2018). Novye tekhnologii platezhei i raschetov kak sposob otmyvaniia deneg [New technologies of payments and settlements as a way of money laundering]. *Perspektivy nauki i obshchestva v usloviakh innovatsionnogo razvitiia: Ahentstvo mezhdunarodnykh yssledovaniy*. pp. 113–115. [in Russian].

5. Myronenko, N.M. (2021). Lehalizatsiia (vidmyvannia) koshtiv – rizni pidkhody do poniattia: biuletyn z obminu dosvidom roboty [Legalization (laundering) of funds – different approaches to the concept: a bulletin on the exchange of work experience]. *MVS Ukraïny*. № 136. pp. 25–28. [in Ukrainian].
6. Poliakova, V.V. (2018). Lehalizatsiia (vidmyvannia) hroshovykh koshtiv ta inshoho mayna, zdobutykh zlochynnym shliakhom (problemy kryminalno-pravovoi kvalifikatsii) [Legalization (laundering) of money and other property obtained by crime (problems of criminal-legal qualification)]. *Naukovi zapysky suchasnykh vchenykh: pratsi 23 mizhnar. nauk.-prakt. konf.* (Vinnytsia, 26 zhovtnia 2018 r.). Vinnytsia, pp. 34–38. [in Ukrainian].
7. Riski otmyvaniia deneg i finansirovaniia terrorizma, sviazannye s COVID-19, i otvetnye mery v oblasti politiki [Money Laundering and Terrorist Financing Risks Associated with COVID-19 and Policy Responses]. *FATF*. Frantsiia, 2020. URL: https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT_rus.pdf [in Russian].
8. Bartlett, M. (2020). How does money laundering work through P2P lending? *Quora*. URL: <https://www.quora.com/How-does-money-laundering-work-through-P2P-lending> [in English].
9. Bitcoin i zlochynnist: yak kryptovaliuty dopomahaiut vidmyvaty hroshi [Bitcoin and crime: how cryptocurrencies help money laundering]. *Finance.ua*. 2018. URL: <https://news.finance.ua/ua/news/-/432104/bitcoin-i-zlochynnist-yak-kryptovalyuty-dopomagayut-vidmyvaty-groshi> [in Ukrainian].
10. Habib, A. (2020). ACFCS Special Contributor Report: Crowdfunding-An unorthodox way of Money Laundering? Definitely maybe. *ACFCS*. URL: <https://www.acfcs.org/acfcs-special-contributor-report-crowdfunding-an-unorthodox-way-of-money-laundering-definitelymaybe/> [in English].
11. MAP FinTech launches AI-powered solution to boost anti-money laundering compliance. *FinTechGlobal*. 2020. URL: <https://member.fintech.global/2020/04/03/map-fintech-launches-ai-powered-solution-to-boost-anti-money-laundering-compliance/> [in English].
12. Metsik, M. (2020). Crowdfunding platforms and anti-money laundering activities. *Estateguru blog*. URL: <https://blog.estateguru.co/crowdfunding-platforms-and-anti-money-laundering-activitiesaml/> [in English].