DOI (Issue): https://doi.org/10.36486/np.2024.3(65) Issue 3-4(65-66) 2024
УДК 336.71:004.7

**Користін Олександр Євгенійович,**
доктор юридичних наук, професор,
заслужений діяч науки і техніки України,
головний науковий співробітник ДНДІ МВС України, м. Київ, Україна,
ORCID ID 0000-0001-9056-5475
**Крищенко Кирило Євгенович,**
кандидат економічних наук, викладач ПВНЗ
«Буковинський університет», м. Чернівці, Україна,
ORCID ID 0009-0007-7145-6709

# СУЧАСНІ ТЕНДЕНЦІЇ ВІДМИВАННЯ КОШТІВ У КІБЕРПРОСТОРІ

*У статті розглянуті сучасні тенденції відмивання коштів у кіберпросторі, акцентуючи на використанні новітніх технологій для здійснення незаконних фінансових операцій. Зловмисники активно використовують криптовалюти, електронні гроші та традиційні інструменти, такі як банківські перекази та платіжні картки, для приховування джерел незаконно отриманих коштів. Основними проблемами є анонімність та глобалізація таких операцій, що значно ускладнює їх виявлення та відслідковування. Стаття також підкреслює важливість посилення міжнародної співпраці, вдосконалення законодавства та технологій моніторингу для боротьби з цією загрозою, що зростає, зокрема у післявоєнний період.*

***Ключові слова:*** *кіберзлочинність, відмиванням коштів, банківський рахунок, криптовалюта, платіжна картка, банківський переказ.*

**Постановка проблеми.** Сучасні розвинені безпекові системи, зокрема й у сфері кібербезпеки, характеризуються новаціями загальнонаукового та спеціального змісту, які створюють можливості передбачення із врахуванням взаємопов'язаних елементів, серед яких одним із основних інструментів є управління ризиками. Наразі, із врахуванням Резолюції генеральної асамблеї ООН та у межах розвитку глобальної культури кібербезпеки, упроваджуються механізми, серед яких одне з ключових місць займає ризик-орієнтований підхід – учасники мають здійснювати періодичну оцінку ризиків з метою виявлення загроз та факторів уразливості, мати належні технології та інструменти контролю для цього з урахуванням значущості інформації і її захисту [1].

Тож, очевидно, реалізуючи державну політику із врахуванням міжнародних стандартів, Україна активно розвивається і в цьому напрямі. Зокрема, у Стратегії національної безпеки України, введеній у дію Указом Президента України від 14 вересня 2020 року № 392/2020 [2], зазначено, що Україна запровадить національну систему стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз, що передбачатиме оцінку ризиків, своєчасну ідентифікацію загроз і визначення вразливостей, а також поширення необхідних знань

і навичок у цій сфері. Про ризик-орієнтований підхід щодо забезпечення кібербезпеки зазначається і в Стратегії кібербезпеки України на період 2021-2025 років [3], а у Плані реалізації Стратегії кібербезпеки [4] (далі – План реалізації Стратегії) чітко визначено завдання: «Впровадити ризик-орієнтований підхід у частині заходів забезпечення кібербезпеки … розробити методики ідентифікації та оцінки кіберризиків …, забезпечити нормативне врегулювання питань щодо впровадження обов›язковості здійснення періодичної оцінки кіберризиків на підставі розроблених методик».

Вочевидь упровадження сучасних методологій потребує відповідного наукового супроводження, до того ж аналіз стратегічного характеру, що базується на емпіричній базі, сформованій широкою експертною думкою, реалізується безпосередньо в межах не лише кримінології, а й соціології, статистики та науки про дані (Data Science), що вимагає дотримання методологічних вимог. Саме тому, на нашу думку, є усі підстави стверджувати, що такі завдання вирішуються переважно в межах прикладного наукового дослідження, із врахуванням дослідницького досвіду та напрацюванням відповідної методології й інструментарію обробки та аналізу великих даних (Big Data).

Науковці ДНДІ МВС України вже не один рік використовують ризик-орієнтований підхід щодо аналізу проблем у сфері безпеки [5–8]. Науковий інтерес завжди викликають зарубіжні новації, упровадження яких в Україні є не лише можливим, а й необхідним процесом. Зокрема, фахівці з кібербезпеки, особливо у сфері правоохоронної діяльності, неодноразово висловлювалися щодо методології Європолу IOCTA [9], яка є головним стратегічним продуктом Європолу, що забезпечує орієнтовану на правоохоронні органи оцінку нових загроз і ключових подій у сфері кіберзлочинності. В аналітичних висновках, окрім загальних характеристик кіберзлочинів, висвітлюються тенденції щодо її поширення, нові форми та напрями, про що свідчать кібератаки. Також зазначається про зростаюче зближення кіберпростору та організованої злочинності тощо.

У дослідженнях багатьох відомих вітчизняних дослідників значна увага приділяється різним проблемам, пов’язаним з розробкою напрямів щодо кібербезпеки, зокрема протидії кіберзлочинності: Бєлякова К.І. [10], Бутузова В.М. [11], Веселової Л.Ю. [12], Гуцалюка М.В. [13; 14], Довганя О.Д. [15], Казмірчук С. [16], Корченка О.Г. [16], Марущака А.І. [17], Гавловського В.Д. [19; 20], Хахановського В.Г. [20], Шеломенцева В.П. [21] та інших.

Водночас, враховуючи стрімкий технологічний розвиток інформаційного простору та цифрового контенту, окремі напрями кіберзлочинів набувають особливого розвитку та поширення і є загрозою не лише сучасного світу, а й майбутніх процесів та суспільних відносин, зокрема це стосується і відмивання коштів у кіберпросторі.

Проблематика сучасних тенденцій відмивання коштів у кіберпросторі є надзвичайно актуальною в умовах цифрової трансформації фінансових та економічних систем. Використання новітніх технологій і інструментів для незаконних фінансових операцій ставить під загрозу стабільність економік, безпеку міжнародних фінансових ринків та ефективність правозахисних органів.

Однією з основних проблем є глобалізація та анонімність операцій у кіберпросторі,

DOI (Issue): https://doi.org/10.36486/np.2024.3(65) Issue 3-4(65-66) 2024

що значно ускладнює виявлення та відслідковування злочинних схем відмивання коштів. Використання криптовалют, анонімних платіжних систем, смарт-контрактів і так званих «міксингових» сервісів для замаскованих трансакцій дозволяє зловмисникам ефективно приховувати джерела незаконно отриманих коштів. Ці технології створюють сприятливі умови для відмивання через численні посередницькі етапи, які важко відслідковувати.

Іншою серйозною проблемою є розвиток фінансових інструментів, таких як фінансові технології (FinTech) і децентралізовані фінансові платформи (DeFi), які часто не мають достатнього рівня регуляції та контролю. Це відкриває нові можливості для фінансових злочинців, адже на таких платформах можна здійснювати транзакції без належної перевірки ідентичності або безпосереднього втручання державних органів.

Зростає також проблема міжнародної співпраці у боротьбі з відмиванням коштів у кіберпросторі. Різні країни мають різні рівні розвитку нормативної бази та протидії фінансовим злочинам, що ускладнює ефективне співробітництво в розслідуванні та викритті злочинних схем. Крім того, зловмисники використовують юридичні прогалини та різницю в законодавствах для переміщення коштів через юрисдикції з менш жорстким контролем.

Нарешті, ще однією проблемою є недостатній рівень обізнаності та технічної підготовки фахівців у сфері кібербезпеки та фінансових інститутів. Багато банків і фінансових установ не мають належних засобів для моніторингу та виявлення підозрілих операцій у реальному часі, що дозволяє злочинцям здійснювати відмивання коштів без серйозних перешкод.

Усе це створює сприятливе середовище для розширення практик відмивання коштів у кіберпросторі, що вимагає не лише вдосконалення технологій, але й зміцнення міжнародної співпраці та адаптації законодавчих ініціатив для ефективної боротьби з цією загрозою.

Метою статті є дослідження проблематики кіберзлочинності з відмивання коштів та специфіки прояву в Україні, враховуючи окремі характеристики та ознаки вчинення цього злочину.

Виклад основного матеріалу. Упродовж 2023–2024 років у співпраці з Департаментом кіберполіції НПУ реалізується НДР щодо аналізу кіберзлочинності в Україні. Серед різних аспектів окремо виділяється проблема відмивання коштів.

Високим рівнем характеризується загроза використання злочинцями механізмів відмивання коштів із застосуванням ІТ-технологій та використанням кіберпростору (48,0 %) (табл. 1). Тренд, використання злочинцями у кіберпросторі та застосування при цьому інформаційно-телекомунікаційних технологій з метою відмивання коштів, за останні роки (зокрема у період воєнного стану) є стабільним без зменшення, а в окремих випадках характеризується підвищенням.



DOI (Article): https://doi.org/10.36486/np.2024.3(65).14

*Таблиця 1*

**Фінансова активність кіберзлочинців**

| ВИДИ ФІНАНСОВОЇ АКТИВНОСТІ КІБЕРЗЛОЧИНЦІВ | Оцінка сучасного поширення | % | Масштаби збільшились | Масштаби не змінилися | Масштаби зменшились | Ризик після війни, % |
|---|---|---|---|---|---|---|
| Шахрайство з платежами | | 67,10 | | | | 45,37 |
| Фінансова активність пов'язана з платежами між злочинцями | | 47,10 | | | | 40,78 |
| Фінансова активність пов'язана з платежами від жертв до злочинців | | 60,90 | | | | 44,42 |
| Відмиванням коштів | | 48,00 | | | | 41,61 |
| Фінансування тероризму | | 32,30 | | | | 36,45 |

Серед фінансових інструментів, що використовуються для відмивання коштів, найбільшим поширенням характеризуються як традиційні – банківські перекази (63,1%) та використання платіжних карток (62,0%), тренд високого рівня за якими зберігається упродовж останніх років та характеризується найвищим рівнем ризику в післявоєнний період (табл. 2), так і більш сучасні – криптовалюти (50,3%), купівля якогось предмету, речі, послуги (48,9%) та електронні гроші (44,6%).

Інші фінансові інструменти також використовуються для відмивання коштів, але відносно зазначених вище видів активність є дещо нижчою: система оплати ваучерами (26,6%) та рахунки мобільних телефонів (40,86%).

Такий же тренд за видами фінансових інструментів, що використовуються для відмивання коштів, зберігався упродовж останніх років. Водночас співвідношення рівнів ризиків, використання різних фінансових інструментів для відмивання коштів залишатиметься сталим і у післявоєнний період.

*Таблиця 2*

**Використання злочинцями механізмів відмивання коштів у кіберпросторі**

| ВІДМИВАННЯ КОШТІВ | Оцінка сучасного поширення | % | Масштаби збільшились | Масштаби не змінилися | Масштаби зменшились | Ризик після війни, % |
|---|---|---|---|---|---|---|
| 8.1. Банківські перекази | | 63,10 | | | | 42,33 |
| 8.2. Платіжні картки | | 62,00 | | | | 42,59 |
| 8.3. Рахунки мобільних телефонів | | 40,86 | | | | 37,31 |
| 8.4. Шляхом купівлі якогось предмету, речі, послуги | | 48,90 | | | | 39,50 |
| 8.5. Система оплати ваучерами | | 26,60 | | | | 32,95 |
| 8.6. Електронні гроші | | 44,60 | | | | 39,34 |
| 8.7. Криптовалюти | | 50,30 | | | | 41,07 |

Здійснюючи платежі з метою відмивання коштів, злочинці переважно використовують грошових мулів (84,50%) та традиційні банківські послуги – банківські карти (83,9%) та банківські перекази (79,8%). Оплата ваучерами використовується порівняно рідше, але все ж достатньо активно (54,8%) (табл. 3).

DOI (Issue): https://doi.org/10.36486/np.2024.3(65) Issue 3-4(65-66) 2024

*Таблиця 3*

**Використання в платежах між злочинцями фінансових механізмів для відмивання коштів**

| ВІДМИВАННЯ КОШТІВ: платежі між злочинцями | Оцінка сучасного поширення | % | Масштаби збільшились | Масштаби не змінилися | Масштаби зменшились | Ризик після війни, % |
|---|---|---|---|---|---|---|
| Банківські перекази | | 79,80 | | | | 50,06 |
| Банківська картка | | 83,90 | | | | 51,50 |
| Грошові мули (дропи) | | 84,50 | | | | 54,54 |
| Система оплати ваучерами | | 54,80 | | | | 42,57 |

Такий же тренд зберігався упродовж останніх років. Водночас співвідношення рівнів ризиків, використання різних фінансових інструментів при розрахунках між злочинцями з метою відмивання коштів залишатиметься сталим і у післявоєнний період. Експертами передбачається, що найвищим рівнем ризику характеризуватиметься використання грошових мулів (дропів) (54,54%). Високим ризиком у майбутньому також оцінюється використання традиційних банківських інструментів: банківських карт (51,5%) та банківських переказів (50,06%).

У характеристиці платежів між злочинцями, з метою відмивання коштів, експерти зазначають про високу фінансову активність використання електронних грошей. Усі системи активно використовуються злочинцями, водночас найчастіше використовуються: EasyPay (84,0%), PayPal (80,1%), а також Webmoney (65,4%), PerfectMoney (64,1%) та Qiwi (62,8%) (табл. 4).

Інші системи електронних грошей також використовуються для платежів між злочинцями, але відносно зазначених вище систем цей рівень є дещо нижчим (52,6%–58,3%).

*Таблиця 4*

**Використання електронних грошей у розрахунках між злочинцями з метою відмивання коштів**

| ВІДМИВАННЯ КОШТІВ: електронні гроші | Оцінка сучасного поширення | % | Масштаби збільшились | Масштаби не змінилися | Масштаби зменшились | Ризик після війни, % |
|---|---|---|---|---|---|---|
| 4.5. Webmoney | | 65,40 | | | | 43,62 |
| 4.6. PerfectMoney | | 64,10 | | | | 43,12 |
| 4.7. ЮMoney | | 58,30 | | | | 40,55 |
| 4.8. Qiwi | | 62,80 | | | | 43,79 |
| 4.9. PayPal | | 80,10 | | | | 46,56 |
| 4.10. Advanced Cash | | 52,60 | | | | 40,96 |
| 4.11. Payeer | | 56,90 | | | | 42,14 |
| 4.12. Skrill | | 53,20 | | | | 40,42 |
| 4.13. EasyPay | | 84,00 | | | | 48,92 |

Такий же тренд за видами систем електронних грошей, що використовуються для здійснення платежів між злочинцями з метою відмивання коштів, з перевагою EasyPay,



DOI (Article): https://doi.org/10.36486/np.2024.3(65).14

PayPal та PerfectMoney зберігався упродовж останніх років. Водночас характерним є певне збільшення масштабів використання електронних грошей з метою відмивання коштів навіть у період воєнного стану.

У післявоєнний період щодо використання електронних грошей для здійснення платежів між злочинцями з метою відмивання коштів експертним середовищем також передбачається висока фінансова активність з перевагою використання: EasyPay (48,92%), PayPal (46,56%) (табл. 4).

Значною активністю у схемах з відмивання коштів характеризується також використання криптовалюти як платежів між злочинцями. Найчастіше використовуються: Bitcoin (91,5%), USDT (82,4%) та Ethereum (76,10%) (табл. 5).

*Таблиця 5*

**Використання криптовалют у розрахунках між злочинцями з метою відмивання коштів**

| ВІДМИВАННЯ КОШТІВ: криптовалюти | Оцінка сучасного поширення | % | Масштаби збільшились | Масштаби не змінилися | Масштаби зменшились | Ризик після війни, % |
|---|---|---|---|---|---|---|
| 4.14. Bitcoin | | 91,50 | | | | 51,29 |
| 4.15. Ethereum | | 76,10 | | | | 47,31 |
| 4.16. Ripple | | 54,50 | | | | 40,67 |
| 4.17. Monero | | 57,40 | | | | 42,76 |
| 4.18. BNB | | 60,80 | | | | 40,70 |
| 4.19. USDT | | 82,40 | | | | 49,46 |
| 4.20. USDC | | 62,50 | | | | 42,64 |
| 4.21. Zcash | | 52,80 | | | | 39,80 |
| 4.22. Dash | | 50,60 | | | | 39,35 |
| 4.23. Litecoin | | 59,10 | | | | 40,61 |

Інші види криптовалют також використовуються, але відносно зазначених вище видів цей рівень є дещо нижчим (50,6%–62,5%).

Такий же тренд за видами криптовалют, що використовуються для здійснення платежів між злочинцями у схемах з відмивання коштів, зберігався упродовж останніх років. Водночас характерним є певне збільшення масштабів використання криптовалют з метою відмивання коштів навіть у період воєнного стану.

У післявоєнний період щодо використання криптовалют для здійснення платежів між злочинцями з метою відмивання коштів експертним середовищем також передбачається високий рівень ризику з перевагою використання Bitcoin (51,29%), USDT (49,46%) та Ethereum (47,31%).

Таким чином, відмивання коштів є розповсюдженим явищем, яке активно використовується злочинцями в кіберпросторі. Традиційні фінансові інструменти, такі як банківські перекази (63,1%) і платіжні картки (62,0%), а також сучасні інструменти, такі як криптовалюти (50,3%) і електронні гроші (44,6%) часто використовуються для цієї мети.

DOI (Issue): https://doi.org/10.36486/np.2024.3(65) Issue 3-4(65-66) 2024

**Висновки.** Відмивання коштів у кіберпросторі є серйозною проблемою, яка активно розвивається в сучасних умовах цифрових трансформацій. Зловмисники використовують як традиційні інструменти, такі як банківські перекази та платіжні картки, так і новітні технології, зокрема криптовалюти та електронні гроші, для здійснення незаконних фінансових операцій. Однією з головних проблем є анонімність і глобалізація цих операцій, що значно ускладнює їх виявлення і відслідковування. Крім того, виникає необхідність у зміцненні міжнародної співпраці та вдосконаленні нормативно-правового регулювання для боротьби з відмиванням коштів.

У статті також аналізуються сучасні тенденції, зокрема стабільне збільшення фінансової активності кіберзлочинців в умовах воєнного стану, коли використовуються як традиційні механізми (банківські карти, перекази), так і новітні фінансові інструменти (криптовалюти, електронні гроші). Прогнозується, що у післявоєнний період найбільшими ризиками будуть характеризуватися саме криптовалюти, зокрема Bitcoin, USDT і Ethereum.

Загалом відмивання коштів у кіберпросторі є постійно зростаючою загрозою, що вимагає не лише вдосконалення технологій моніторингу та контролю, але й адаптації законодавчих ініціатив, щоб забезпечити ефективну боротьбу з цими злочинами.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Резолюция Генеральной Ассамблеи ООН 57/329, принятая на 78 пленарном заседании 57-й сессии. 20 декабря 2002 года. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement (дата звернення: 06.08.2024).

2. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»»: Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 06.08.2024).

3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 05.08.2024).

4. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України»»: Указ Президента України від 01 лютого 2022 року № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/37/2022#Text (дата звернення: 06.08.2024).

5. *Kovalchuk T.I., Korystin O.Y., Sviridyuk N.P.* Hybrid threats in the civil security sector in Ukraine. *Problems of Legality.* 2019. № 147. P. 163–175. DOI: https://doi.org/10.21564/2414-990x.147.180550.

6. *Oleksandr Korystin, Nataliia Svyrydiuk, Volodymyr Tkachenko.* Fiscal security of the state considering threats of macroeconomic nature. Proceedings of the international conference on business, accounting, management, banking, economic security and legal regulation research (BAMBEL2021). *Atlantis Press* – now part of *Springer Nature. Series: Advances in Economics, Business and Management Research.* Vol. 188. P. 65-69. DOI: https://doi.org/10.2991/AEBMR.K.210826.012

7. *Користін О.Є., Цюприк І.В., Свиридюк Н.П., Прокоф'єфа-Янчиленко Д.М.* Оцінювання ризиків розвитку системи кримінальної юстиції України. *Наука і правоохорона.* 2021. № 2. С. 108–116. DOI: https://doi.org/10.36486/np.2021.2(52)

8. *Користін О.Є., Свиридюк Н.П.* Оцінювання загроз у сфері лісового господарства України. *Наука і правоохорона.* 2023. № 1. С. 145–153. DOI: https: //doi.org/10.36486/np.2023.1(59).

9. Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021. Publications Office of the European Union. Luxembourg. 2021.

10. *Бєляков К.І.* Інформація в праві: теорія і практика: монографія. Київ: Видавництво «КВІЦ», 2006. 116 с.

11. *Бутузов В.М.* Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія. Київ: КИТ, 2010. 408 с.

12. *Користін О.Є., Веселова Л.Ю.* Ризикорієнтованість кібербезпеки. *Наука і правоохоронна.* 2021. № 3. С. 16–23.

13. *Гуцалюк М.В.* Сучасні тенденції організованої кіберзлочинності. *Інформація і право.* 2019. № 1(28). С. 118-128.

14. *Гуцалюк М.В., Хахановський В.Г.* Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник.* 2020. 31(1). С. 13–19. DOI: https://doi.org/10.37025/1992-4437/2019-31-1-13.

15. *Довгань О.Д., Доронін І.М.* Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. Київ: Видавничий дім «АртЕк», 2017. 107 с.

16. *Корченко О., Казмірчук С., Ахметов Б.* Прикладні системи оцінювання ризиків інформаційної безпеки: монографія, Київ: ЦП Компринт, 2017. 435 с.

17. *Марущак А.І.* Інформаційні ресурси держави: зміст та проблема захисту. *Правова інформатика.* 2009. № 1(21). С. 65–71.

18. *Погорецький М.А., Шеломенцев В.П.* Комп'ютерна система як знаряддя вчинення злочину. *Вісник Харківського національного університету ім. В. М. Каразіна. Серія «Право».* 2009. № 872. Вип. 6. С. 117–121.

19. *Таран О.В., Гавловський В.Д.* Організована кіберзлочинність в Україні: проблеми формування офіційної статистики та її аналізу. *Інформація і право.* 2021. № 4(39). С. 193-201.

20. *Хахановський В.Г., Гавловський В.Д.* Тлумачення та класифікація кримінальних правопорушень як кіберзлочинів. *Інформація і право.* 2020. № 2(33). С. 99–110.

21. *Шеломенцев В.П.* Організована кіберзлочинність: до визначення поняття. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2009. Вип. 21. С. 314–322.

## REFERENCES

1. Rezoliutsiia Heneralnoi Assamblei OON 57/329. "UN General Assembly Resolution 57/329, adopted at the 78th plenary meeting of the 57th session. December 20, 2002. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement (Date of Application: 06.08.2024).

2. Pro rishennia Rady natsionalnoi bezpeky i oborony «Pro Stratehiiu natsionalnoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy. "On the decision of the National Security and Defense Council of Ukraine of September 14, 2020 'On the National Security Strategy of Ukraine'": Decree of the President of Ukraine of September 14, 2020 No. 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (Date of Application: 06.08.2024) [in Ukrainian].

3. Pro rishennia Rady natsionalnoi bezpeky i oborony «Pro Stratehiiu kiberbezpeky Ukrainy»: Ukaz Prezydenta Ukrainy. "On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 'On the Cybersecurity Strategy of Ukraine'": Decree of the President of Ukraine dated August 26, 2021 No. 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013. (Date of Application: 05.08.2024) [in Ukrainian].

4. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy «Pro Plan realizatsii Stratehii kiberbezpeky Ukrainy»: Ukaz Prezydenta Ukrainy. "On the decision of the National Security and Defense Council of Ukraine dated December 30, 2021 On the Implementation Plan of the Cybersecurity Strategy of Ukraine'": Decree of the President of Ukraine dated February 01, 2022 No. 37/2022. URL: https://zakon.rada.gov.ua/laws/show/37/2022#Text. (Date of Application: 06.08.2024) [in Ukrainian].

DOI (Issue): https://doi.org/10.36486/np.2024.3(65) Issue 3-4(65-66) 2024

5. *Kovalchuk, T.I., Korystin, O.Y. and Sviridiuk N.P.* (2019). Hybrid threats in the civil security sector in Ukraine. *Problems of Legality, 147,* 163-175. DOI: https://doi.org/10.21564/2414-990x.147.180550 [in English].

6. *Oleksandr, Korystin, Nataliia, Svyrydiuk and Volodymyr, Tkachenko* (2021). Fiscal security of the state considering threats of macroeconomic nature. Proceedings of the international conference on business, accounting, management, banking, economic security and legal regulation research (BAMBEL2021). *Atlantis Press* – now part of *Springer Nature. Series: Advances in Economics, Business and Management Research, 188,* 65-69. DOI: https://doi.org/10.2991/AEBMR.K.210826.012 [in English].

7. *Korystin, O.Ye., Tsiupryk, I.V., Svyrydiuk, N.P. and Prokofiefa-Yanchylenko, D.M.* (2021). Otsiniuvannia ryzykiv rozvytku systemy kryminalnoi yustytsii Ukrainy. "Risk assessment of the development of the criminal justice system of Ukraine". *Nauka i Pravookhorona, 2,* 108-116. DOI: https://doi.org/10.36486/np.2021.2(52) [in Ukrainian].

8. *Korystin, O.Ye., Svyrydiuk, N.P.* (2023). Otsiniuvannia zahroz u sferi lisovoho hospodarstva Ukrainy. "Threat assessment in the forestry sector of Ukraine". *Nauka i Pravookhorona, 1,* 145-153. DOI: https://doi.org/10.36486/np.2023.1(59) [in Ukrainian].

9. Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021. Publications Office of the European Union. Luxembourg. 2021. [in English].

10. *Bieliakov, K.I.* (2006). Informatsiia v pravi: teoriia i praktyka. "Information in law: theory and practice": monograph. Kyiv: Publishing House "KVITs". 116 p. [in Ukrainian].

11. *Butuzov, V.M.* (2010). Protydiia kompiuternii zlochynnosti v Ukraini (systemno-strukturnyi analiz). "Counteraction to computer crime in Ukraine (systemic and structural analysis)": monograph. Kyiv: KYT. 408 p. [in Ukrainian].

12. *Korystin, O.Ye., Veselova, L.Yu.* (2021). Ryzykoriientovanist kiberbezpeky. "Risk orientation of cybersecurity". *Nauka i Pravookhoronna, 3,* 16-23 [in Ukrainian].

13. *Hutsaliuk, M.V.* (2019). Suchasni tendentsii orhanizovanoi kiberzlochynnosti. "Modern trends in organized cybercrime". *Information and Law, 1(28),* 118-128 [in Ukrainian].

14. *Hutsaliuk, M.V., Khakhanovskyi, V.H.* (2020). Osoblyvosti vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh. "Peculiarities of using electronic (digital) evidence in criminal proceedings". *Forensic Bulletin, 31(1),* 13-19. DOI:https://doi.org/10.37025/1992-4437/2019-31-1-13 [in Ukrainian].

15. *Dovhan, O.D., Doronin, I.M*. (2017). Eskalatsiia kiberzahroz natsionalnym interesam Ukrainy ta pravovi aspekty kiberzakhystu. "Escalation of cyber threats to the national interests of Ukraine and legal aspects of cyber protection": monograph. Kyiv: Publishing House "ArtEk". 107 p. [in Ukrainian].

16. *Korchenko, O., Kazmirchuk, S. and Akhmetov, B.* (2017). Prykladni systemy otsiniuvannia ryzykiv informatsiinoi bezpeky. "Applied systems for assessing information security risks": monograph. Kyiv: TsP Komprynt. 435 p. [in Ukrainian].

17. *Marushchak, A.I.* (2009). Informatsiini resursy derzhavy: zmist ta problema zakhystu. "State information resources: content and protection problem". *Legal Informatics, 1(21),* 65-71 [in Ukrainian].

18. *Pohoretskyi, M.A., Shelomentsev, V.P.* (2009). Kompiuterna systema yak znariaddia vchynennia zlochynu. "Computer system as a tool for committing a crime. The *Journal of V.N. Karazin Kharkiv National University. Series "Law", 872(6),* 117-121 [in Ukrainian].

19. *Taran, O.V., Havlovskyi, V.D.* (2021). Orhanizovana kiberzlochynnist v Ukraini: problemy formuvannia ofitsiinoi statystyky ta yii analizu. "Organized cybercrime in Ukraine: problems of forming official statistics and its analysis". *Information and Law, 39,* 193-201 [in Ukrainian].

20. *Khakhanovskyi, V.H., Havlovskyi, V.D.* (2020). Tlumachennia ta klasyfikatsiia kryminalnykh pravoporushen yak kiberzlochyniv. "Interpretation and classification of criminal offenses as cybercrimes". *Information and Law, 2(33),* 99-110 [in Ukrainian].



DOI (Article): https://doi.org/10.36486/np.2024.3(65).14
Issue 3-4(65-66) 2024 https://naukaipravoohorona.com/

21. *Shelomentsev, V.P.* (2009). Orhanizovana kiberzlochynnist: do vyznachennia poniattia. "Organized cybercrime: to define the concept". *Fight Against Organized Crime and Corruption (Theory and Practice), 21,* 314-322 [in Ukrainian].

UDC 336.71:004.7

**Korystin Oleksandr,**
Doctor of Juridical Sciences, Professor,
Honored Worker of Science and Technology of Ukraine,
State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0001-9056-5475
**Kryshchenko Kyrylo,**
Candidate of Economical Sciences, Lecturer of the
Bukovinian University, Chernivtsi, Ukraine,
ORCID ID 0009-0007-7145-6709

## CURRENT TRENDS OF MONEY LAUNDERING IN CYBERSPACE

The article is dedicated to examining the current trends in money laundering in cyberspace, which is a significant problem for financial stability and security at the international level. The article emphasizes the growing use of new technologies and financial instruments to carry out illegal financial transactions, particularly cryptocurrencies, electronic money, as well as traditional mechanisms such as bank transfers and payment cards. These instruments allow criminals to disguise the sources of illegally obtained funds, creating significant challenges for detecting and tracking criminal schemes. The anonymity of such operations and the globalization of financial flows contribute to the increasing scale of money laundering, posing a serious threat to the stability of financial systems and international markets.

The article also focuses on the development of financial technologies (FinTech) and decentralized financial platforms (DeFi), which are largely unregulated, creating additional opportunities for illegal financial transactions. Criminals use these platforms for anonymous transactions, making it more difficult for law enforcement agencies and financial institutions to combat money laundering. Furthermore, the article discusses the need to strengthen international cooperation and improve legislation for effective counteraction against cybercrime and financial crimes.

The research underscores the importance of improving monitoring technologies and implementing effective methods for detecting suspicious transactions in real-time. The authors have identified a primary challenge, namely the inadequate level of awareness and technical training of cybersecurity professionals and financial institutions, which allows criminals to carry out money laundering without significant obstacles. It is forecasted that in the post-war period, the greatest risks will be associated with cryptocurrencies, particularly Bitcoin, USDT, and Ethereum, which have become popular among criminals for money laundering.

DOI (Issue): https://doi.org/10.36486/np.2024.3(65) Issue 3-4(65-66) 2024

In conclusion, money laundering in cyberspace is a continuously growing problem that requires not only the improvement of technologies but also the integration of international standards, the strengthening of control, and the adaption of legislative initiatives to effectively combat this threat.

**Keywords:** cybercrime, money laundering, bank account, cryptocurrency, payment card, bank transfer.

Отримано 11.09.2024