КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.24.150160
УДК 004.056

**Борсуковська Вікторія Юріївна**
юрисконсульт з питань протидії відмиванню
коштів та фінансуванню тероризму
ПрАТ «Київстар», Київ, Україна
ORCID ID: 0000-0002-4929-6987
*v.barsik@gmail.com*

**Борсуковський Юрій Володимирович**
к.т.н., доцент
Державний університет інформаційно-комунікаційних
технологій, Київ, Україна
ORCID ID: 0000-0003-1973-2386
*BYurii@duikt.edu.ua*

# ФІНАНСОВІ ЗЛОЧИНИ В КІБЕРПРОСТОРІ: РИЗИКИ ТА ЗАГРОЗИ ЛЕГАЛІЗАЦІЇ НЕЗАКОННИХ ФІНАНСОВИХ АКТИВІВ

**Анотація.** В цій статті розглянуті питання протидії фінансовим злочинам в кіберпросторі. Кібервідмивання становить значну загрозу для світової фінансової системи, оскільки дозволяє злочинцям приховувати та використовувати доходи від своєї незаконної діяльності. Це також створює виклик для правоохоронних органів, які повинні адаптувати свої методи, щоб не відставати від цифрового ландшафту, що постійно розвивається. Розглянуто питання використання сучасних технологій для здійснення кіберзлочинів з метою порушення, руйнування або створення загроз критичній інфраструктурі та/або поширення страху та паніки з кінцевою метою заподіяння фізичної чи економічної шкоди суспільству чи його народу. Проаналізовано зв'язок з легалізацією фінансових активів у кіберпросторі і кібертероризму. Зазначено, що новий тип тероризму використовує взаємопов'язаність і вразливість цифрових систем і мереж сучасного суспільства для досягнення своїх зловмисних цілей. Протягом останнього десятиліття загроза кібертероризму стає все більш актуальною проблемою як для урядів, так і для бізнесу. Оскільки технології продовжують розвиватися, а все більше ресурсів критично-важливих інфраструктур підключено до світової цифрової мережі, ймовірність того, що кібератаки можуть завдати серйозної шкоди та збоїв, більша, ніж будь-коли раніше. Використання цифрових валют ще більше загострює та поглиблює дані проблеми. Створення цифрових валют на рівні держав дозволяє реалізовувати процедури прямої торгівлі з країнами, які приймають дані платежі без конвертації їх у загально прийняті світові валюти. Це дає можливість створювати механізми для приховування джерела транзакцій. Відповідно постають питання розробки методів і алгоритмів виявлення і проактивної протидії фінансовим злочинам в кіберпросторі, як складової частини загальної системи кібербезпеки інформаційних ресурсів.

**Ключові слова:** кібервідмивання; предикатний злочин; кібертероризм; кібератака; кібербезпека.

## ВСТУП

Розвиток глобальної інтернет-мережі та цифрових технологій приніс багато переваг і зручностей у повсякденне життя користувачів цифрового світу, від здійснення онлайн-покупок до спілкування у соціальних мережах. Однак, інтенсивна цифровізація повсякденного життя разом із зручностями також відкрила двері для нового виду злочинної діяльності, направленої на легалізацію незаконно здобутих фінансових коштів.

Процес легалізації кримінальних коштів, починаючи від звичайного інтернет-шахрайства і закінчуючи незаконною торгівлею в цифровому просторі, зазвичай

включає кілька етапів — це розміщення нелегальних коштів у віртуальному просторі, нашарування та інтеграція цих віртуальних фінансових ресурсів, як процес традиційного відмивання кримінальних коштів. На етапі розміщення незаконні кошти вводяться в цифрову систему, часто через анонімні онлайн-транзакції. На етапі нашарування кошти переміщуються та маскуються за допомогою кількох транзакцій, часто в різних юрисдикціях та валютах. На етапі інтеграції кошти знову вводяться в легітимну фінансову систему, як правило, шляхом купівлі активів або інвестицій.

Одним із найпоширеніших методів кібервідмивання є віртуальні валюти, які дозволяють здійснювати анонімні транзакції щодо яких неможливо відстежити власника. Злочинці можуть використовувати ці валюти для покупки товарів і послуг в Інтернеті, переказу коштів через кордони та конвертації отриманих коштів назад у традиційні валюти, не залишаючи цифрового сліду. Інша техніка полягає у використанні анонімних інструментів зв'язку та шифрування, які дозволяють злочинцям спілкуватися та переказувати кошти непомітно. Вони також можуть використовувати складні методи, такі як послуги «змішування», які інтегрують кошти кількох транзакцій, щоб ускладнити відстеження першоджерела.

Все це вимагає створення системних підходів для боротьби з легалізацією незаконно здобутих фінансових активів в загальних процесах забезпечення безпеки інформаційних ресурсів держав, комерційних структур, приватних осіб тощо.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

**Поняття кібервідмивання.** Визначення кібервідмивання має обов'язково відображати його елементи як відмивання коштів, так і кіберзлочинності і має на меті створення відповідних когнітивних моделей в системах інформаційної безпеки.

Відмивання коштів — це складний, а іноді і не дуже, процес приховування коштів, майна, прав та інших цінностей, отриманих в результаті вчинення протиправних дій, тобто це результат злочину. Це процесний злочин, який не має на меті нанесення шкоди життю або здоров'ю особи чи власності, метою його є зловживання недосконалостями законів та їх використання із злочинною метою для власної вигоди і збагачення. Подібно до логіки, що лежить в основі інших процесуальних злочинів, таких як перешкоджання здійсненню правосуддя, неповага до суду та лжесвідчення, відмивання коштів здійснюється шляхом маскування або приховування предикатного злочину через мережу обманних та обхідних процесів.

Однак кібервідмивання це вже наступний щабель у практиці відмивання коштів, який включає технологічний аспект та перетинається з широким простором кіберзлочинності. Кіберзлочин можна визначити як кримінально карне діяння, вчинене з використанням автоматичного електронного пристрою, який виконує математичні або логічні функції, наприклад, комп'ютера. Взаємодія з кібервідмиванням відбувається, коли результатом вищевказаної «дії» є безпосередньо залучення автоматичного електронного пристрою для здійснення відмиванням коштів в його класичному розумінні [1].

З огляду на викладене, можна визначити кібервідмивання у наступний спосіб:

Кібервідмивання — це використання комп'ютерного обладнання для створення транзакцій або відносин, пов'язаних із майном, коштами або вигодою, як матеріальною, так і нематеріальною, отриманих в результаті злочинної діяльності, та створення максимальної видимості їх законного походження.

Незважаючи на те, що комп'ютерне обладнання є інструментом, безпосереднім майданчиком операційної діяльності, як законної, так і незаконної, залишається глобальна інтернет-мережа. Ось чому глобальна інтернет-мережа повинна стати основним джерелом дослідження для виявлення та блокування слабких місць, які можуть використовуватися злочинцями для відмивання коштів та вчинення інших злочинів [11], [12].

**Загроза кібервідмивання.** Для розуміння концепції кібервідмивання необхідно звернутися до історії його розвитку. Феномен кібервідмивання виник з появою глобальної інтернет-мережі, яку злочинці почали використовувати як новітній інструмент відмивання коштів, зручний, іноді недостатньо врегульований, а іноді і зовсім не врегульований та, у своїй більшості, анонімний або максимально прихований.

Сучасне комп'ютерне обладнання розроблене таким чином, що воно здатне обробляти дані з надзвичайною швидкістю завдяки можливостям центрального процесора комп'ютера (CPU). Додатковим визначником швидкості також є оперативна пам'ять комп'ютера (RAM) і графічна карта. Перший відноситься до депозитарію, де використовуються або зберігаються поточні файли. Отже, з дуже швидкою оперативною пам'яттю можна гарантувати легкий доступ до своїх файлів. З іншого боку, відеокарта — це апаратне забезпечення, яке обробляє графіку та дозволяє прискорювати обчислення за рахунок потужних графічних процесорів. За допомогою сучасної відеокарти за секунду можна обробляти більше графічних зображень та цифрових даних, що має вирішальне значення для комп'ютерних транзакцій. Швидкість комп'ютерного обладнання додатково доповнюється не менш швидким інтернет-сервісом і доступом до ресурсів хмарних технологій. Завдяки переходу від комутованого доступу до широкосмугового доступу до мережі Інтернет (останній у середньому становить близько чотирьох мегабайт на секунду, на відміну від 60 кілобайт на секунду в першому) гарантується висока швидкість передачі даних, що представляє особливий інтерес для «відмивачів» коштів, які перш за все цінують швидкість у проведенні своїх операцій.

Звичайно, не слід вважати, що кібервідмивання пов'язане лише з цими основними характеристиками технології і без цих функцій поняття кібервідмивання не існуватиме. Іншим рушійним механізмом питання кібервідмивання є доступ до глобальної інтернет-мережі. Фактично глобальна інтернет-мережа є віртуальним майданчиком для кібервідмивання. Розвинувшись на основі кількох військових проектів уряду США наприкінці 60-х років XX століття, сьогодні глобальна інтернет-мережа надає найбільше сприяння кібервідмиванню, оскільки глобальна інтернет-мережа стала звичайною «розкішшю» для всіх, враховуючи її усюдисущу природу та присутність [2]. На початку свого розповсюдження, тобто в 90-х роках XX століття, Інтернет був певним чином доволі доступний підприємствам і домашнім господарствам, головним чином у США та Великобританії. Ця популярність була заснована на підвищенні обізнаності про функціональні можливості глобальної інтернет-мережі та її безмежної ємності. Тому можна сказати, що кібервідмивання походить від глобалізації Інтернету. Наразі, залишилися в історії часи, коли лише еліта мала доступ до такого багатства як інформація. Сьогодні, завдяки розвитку глобальної інтернет-мережі, світ став глобальним селом. За виключенням певної людської діяльності, якою не можна займатися в Інтернеті, як-от їсти та пити (принаймні поки), багато речей можна зробити в Інтернеті.

Доступ до глобальної інтернет-мережі продовжує зростати. Статистичні дані показують, що у минулому столітті ця цифра становила лише 360 мільйонів, а станом на січень 2023 року це число зросло до 5,16 мільярдів користувачів інтернету. Це означає, що 64,4% світового населення мають доступ до інтернету. Незважаючи на уповільнення,

поточні тенденції свідчать про те, що до кінця 2023 року майже 2/3 населення світу буде підключено до Інтернету [3].

Той факт, що повсякденне життя людини в основному починає обертатися навколо глобальної інтернет-мережі, цей ресурс стає повсякденним інструментом для багатьох людських дій. Доступність до глобальної інтернет-мережі стало темою для гарячих суперечок, і дебати навіть перемістилися в сферу права, що породило численні дискусії. У 2003 році під час Всесвітнього саміту Організації Об'єднаних Націй з питань інформаційного суспільства було запропоновано закріпити доступ до мережі Інтернет як фундаментальне право людини. Відтоді кілька країн, таких як Фінляндія, Франція, Греція, Іспанія та Естонія, зробили доступ до Інтернету частиною основних фундаментальних прав людини.

Це свідчить про серйозність і важливість питання доступності Інтернету. В наш час доступ до глобальної інтернет-мережі є надзвичайно важливим для всіх людей. Доступ до Інтернету стоїть вже майже на одному щаблі з правом на життя. Міжнародний союз електрозв'язку («International Telecommunication Union — MCE») також приєднався до кампанії з глобалізації доступу до Інтернету та очолив декілька проектів на багатьох континентах для досягнення цієї мети. Європейський Союз («European Union — ЕС») також відповідально ставиться до питання забезпечення захисту права на доступ до Інтернету. З цією метою у грудні 2023 року постійні представники держав-членів Європейського Союзу досягли попередньої згоди щодо регламенту про кіберсолідарність, який передбачає посилене реагування на кіберінциденти й кіберспівпрацю в ЄС [9].

Іншими країнами, які поділяють це поняття, але які ще не закріпили його як фундаментальне право людини, є Південна Корея, Мексика, Бразилія, Туреччина та Нігерія. Результати опитування показали, що ці країни рішуче виступають проти урядового регулювання Інтернету, хоча є країни Азії, які не погоджуються з таким підходом.

Крім того, з роками свого розвитку глобальна інтернет-мережа стала не тільки доступною, але й зручною, особливо з появою хмарних рішень. Останнє означає все, що передбачає надання розміщених послуг через інтернет-мережу і працює таким чином, що можна отримати доступ до даних/інформації, що міститься в хмарному сховищі в глобальній інтернет-мережі, за допомогою будь-якого комп'ютерного обладнання і, практично, без будь-якої територіальної прив'язки. Більше того, у сучасну епоху комп'ютер не обов'язково повинен бути настільним або портативним; також це може бути телефон або будь-який персональний цифровий помічник/планшет.

Один дуже яскравий факт полягає в тому, що як показує статистика, легкий доступ до Інтернету в глобальному масштабі продовжить зростати протягом наступних років. Негативною стороною є те, що без дієвого регуляторного поля для мінімізації зловживань, особливо для цілей відмивання коштів, явища кібервідмивання та кіберзлочинності неминуче зростатимуть.

Ще однією проблемою кібервідмивання є поняття анонімності. Питання анонімності завжди було предметом суперечок, задовго до того, як дискусія перейшла в площину анонімності в Інтернеті. Спочатку питання анонімності було протиставлено фундаментальному праву людини на свободу вираження поглядів, свободу слова, приватне життя тощо. Після появи і широкого використання ресурсів інтернет-мережі, ця дискусія анонімності одразу мігрувала в електронний простір. Інтернет має властивість анонімності, оскільки дозволяє особам вчиняти дії, не розкриваючи свою справжню особу або ж сприяє можливості уникнення прямого відстеження. Однак поняття анонімності в цьому контексті відрізняється від деяких його варіантів, таких як використання нікнеймів та псевдонімів. Останні форми анонімності, якщо вони

використовуються в Інтернеті, можуть мати на меті і хороші цілі. Серед деяких переваг анонімності є: її можливе використання людьми під час репресивного політичного режиму, щоб висловити свою думку; її можна використовувати для розголошення інформації надзвичайно особистого характеру, наприклад проблем, пов'язаних із здоров'ям. Анонімність могла би служити платформою для висловлення думок, таким чином сприяючи паритету та роблячи атрибути статі та раси несуттєвими. На жаль, кілька переваг, пов'язаних з анонімністю в глобальній інтернет-мережі, затьмарюються більш явними недоліками. Із нескінченного переліку недоліків анонімності, злочинець може згенерувати ідеальну павутину транзакцій через глобальну інтернет-мережу, знищивши таким чином усі сліди предикатного злочинного акту. По суті, це і є кібервідмивання. Враховуючи численні небезпеки, які створює глобальна інтернет-мережа через її функцію анонімності, деякі з експертів вважають за доцільне проведення так званої «реконструкції» або «реструктуризації» Інтернету для створення універсальної ідентифікації, і таким чином повністю знищити поняття анонімності, яка насьогодні формує серцевину сутності глобальної інтернет-мережі.

Ще одною наріжною проблемою кібервідмивання є безмежні кордони всесвітньої інтернет-мережі. Протягом більшої частини свого існування глобальна інтернет-мережа зазнала спорадичних змін у розвитку, але постійним фактором її еволюції є її безперервна природа звуження світу та його розміщення в одному просторі. Спосіб, у який інформація доступна через інтернет-мережу, легко долає фізичні та електронні бар'єри. Безсумнівно, феномен Інтернету визначає сучасність. Однак така зручність дивує та продовжує викликати цікавість. З одного боку, багато хто дивується, чому сучасні уряди надто прискіпливі щодо цензури в Інтернеті, тоді як з іншого боку основоположне право на доступ до інформації рішуче відстоюється. Наприклад, поточна ситуація в Італії, де на ринку присутня гігантська інтернет-компанія Google. Італійський Уряд визнав YouTube телевізійною станцією, на яку поширюються телевізійні правила. Це означає, що Google сплачує податки як телевізійний мовник і несе відповідальність за свій контент [4]. YouTube було заборонено в кількох країнах, таких як Китай і Марокко, оскільки люди часто публікують відео, які уряди цих країн вважали образливими та такими, що можуть викликати антиурядові протести. Крім того, у січні 2010 року з цієї ж причини уряд Лівії заблокував доступ до YouTube.

Однак наведені вище випадки є лише поодинокими прикладами. Факт залишається фактом: обмін інформацією в глобальній інтернет-мережі продовжує зростати, і деякі уряди, серед яких США та Великобританія, все ще заохочують антицензуру та рішуче відстоюють права на свободу вираження думок. Таким чином, можна сказати, що наразі ваги схиляються на користь безмежного інтернет-середовища. Складність цього питання виражається наступним чином:

Складність полягає в тому, що хоча країни і розуміють переваги обміну інформацією в глобальній інтернет-мережі, але одночасно вони вбачають зростання цифрового тероризму, широкомасштабної злочинності, шахрайства, спаму, переслідування та порнографії [10]. Делікатна частина дискусії, як і всі дебати про цензуру, полягає не в тому, чи потрібно виключити деякі з цих областей з глобальної інтернет-мережі, а в тому, де проводиться межа між законною загрозою або ризиком безпеки та тим, що уряди країн беруть на себе роль національних політичних, моральних і етичних наглядачів [5].

Розповсюдження інформації через глобальну інтернет-мережу і легкість отримання доступу до неї призвели як до добра, так і до зла, причому останнє проявляється у формі кіберзлочинів, які надалі трансформуються у кібервідмивання.

**Класифікація кібервідмивання.** Кібервідмивання перетинає дві різні сфери злочинності — кіберзлочинність з одного боку, та відмивання коштів з іншого. Це робить його гібридним злочином, який, в свою чергу, ставить запитання: як слід розглядати кібервідмивання та до якої категорії злочинів його віднести? У рамках прагнення зрозуміти предмет, для цілей створення відповідної правової бази, необхідно побачити кібервідмивання через правильну призму. Тому з самого початку кібервідмивання необхідно встановити у правильні рамки. Не встановивши параметрів кібервідмивання, можна заплутатися на цьому шляху, оскільки саме поняття може бути сконцентровано в одній великій концептуальній розмитості [6].

**Кібервідмивання як різновид кіберзлочинності.** Чи слід розглядати кібервідмивання як частину кіберзлочинності? Якщо кібервідмивання справді розглядається як різновид кіберзлочинності, це означатиме, що воно прямо входить до сфери кіберзлочинності, без елемента відмивання коштів. Якщо це так, можливо, доведеться звернути увагу виключно на сферу інформатики, щоб знайти для неї регулятивні заходи.

Однак такий підхід не може бути цілком прийнятним. Хоча загальновизнано, що кібервідмивання має коріння в кіберзлочинності, не можна випускати з уваги й основний елемент відмивання коштів. Отже, суттю злочину є відмивання коштів з технологічним аспектом.

**Кібервідмивання як техніка відмивання коштів.** Інше популярне спрямування думок щодо кібервідмивання розглядає його не лише як елемент відмивання коштів, а виключно як звичайну техніку відмивання коштів. Тобто, якщо для відмивання коштів злочинець використовує інтернет-мережу, одразу і швидко робиться висновок, що відмивання коштів було здійснено за допомогою цієї техніки. Це уявлення може бути обґрунтованим, якщо поглянути на широку концепцію відмивання коштів, яка включає в себе кілька інших аспектів, наприклад, відмивання коштів у торгівлі.

Тим не менш, було б абсолютно неправильно визнати, що кібервідмивання є лише технікою відмивання коштів. Розглядати щось як «техніку» іншого означало б, що остання є засобом досягнення мети, і, мабуть, що вона не може стояти сама по собі. Що стосується кібервідмивання, той факт, що злочинець використовує технологічні ресурси, не робить такі ресурси просто інструментом відмивання коштів для звичайного підприємства; навпаки, це робить діяльність злочинця компанією з відмивання коштів.

**Кібервідмивання — «мистецтво відмивання».** Тож яким може бути правильне концептуальне поняття кібервідмивання? Відповідь лежить в основі самого злочину, яким є відмивання коштів. Досить хитра відповідь полягає в тому, що кібервідмивання — це відмивання коштів, яке відбувається на більш просунутому рівні, враховуючи його високотехнологічну складову. Хоча це збігається з концепцією кіберзлочинності, не слід розглядати його повністю в цьому світлі. Можна стверджувати, що серйозність проблеми кібервідмивання, яка вже втілює величезну вагу відмивання коштів, перевищує загалом тяжкість інших видів кіберзлочинів. Важливо знати правильну категорію, до якої потрапляє кібервідмивання, оскільки розуміння чітких рамок визначатиме вид відповідальності, яку воно створює. Визнавши, що кібервідмивання є відмиванням коштів, основною відповідальністю буде відповідальність за відмивання коштів. Однак кібервідмивання унікальне тим фактом, що воно, ймовірно, створить субсидіарну або допоміжну відповідальність для злочинця, крім відповідальності за відмивання коштів. Це може призвести до зобов’язань за широким поняттям кіберзлочинності або інших різновидів кіберзлочинності в юрисдикціях, де такі злочини визнаються карними. Така допоміжна відповідальність відрізняється від традиційних предикатних злочинів, які

зазвичай встановлюють відповідальність за злочин відмивання коштів. Наприклад, кібервідмивача, ймовірно, буде визнано відповідальним за такі злочини, як хакерство чи кібервандалізм, обидва з яких, але не обов'язково, можуть бути предикатними злочинами для відмивання коштів.

Ще одним моментом, який підтверджує проблему кібервідмивання, є аспект судового переслідування. Коли прокурор переслідує осіб, які брали участь у діяльності з кібервідмивання, назва злочину, яка відображається в обвинуваченні — це «відмивання коштів», а не кібервідмивання. По суті, кібервідмивання не є окремим злочином, але все ж лишається злочином відмивання коштів з використанням високотехнологічних інструментів. Суть відмивання не змінюється, змінюються лише засоби та інструменти досягнення злочинної мети. Сумна реальність полягає в тому, що серйозність проблеми кібервідмивання призводить до загострення поточної проблеми відмивання коштів і, відповідно, кібервідмивання є юридичною проблемою з дуже складними правовими наслідками.

**Розповсюджені методи кібервідмивання.** Незважаючи на те, що практично кожна діяльність в мережі інтернет-мережі може бути використана для кібервідмивання коштів, в останній час уряди багатьох країн почали більш ретельно вивчати наступні методи, які спричиняють найбільшу занепокоєність [7], [11]:

***Алгоритми машинного навчання*** — кіберзлочинці успішно використовують машинне навчання для створення схем або пошуку слабких місць у діючих системах захисту, що дозволяє їм безперешкодно входити в фінансові системи без великих побоювань бути виявленими.

***Використання «мулових» рахунків*** — ідея не нова, але суттєво вдосконалена в частині використання в цифровому просторі. Зазвичай це рахунки відкриті на численні імена, основною метою яких є використання виключно з метою відмивання коштів.

***Подарункові картки та ваучери*** — це ідеальний варіант анонімних покупок за готівкові брудні кошти, які в подальшому можуть бути перепродані в глобальній інтернет-мережі вже за законні кошти не викликаючи жодних підозр.

***Фіктивні рахунки*** — можуть бути виставлені будь-якими компаніями за неіснуючі/ненадані послуги або товари, а оплата таких рахунків суттєво допомагає у відмиванні коштів.

**Як боротися з кібервідмиванням.** Боротьба з кібервідмиванням потребує нестандартного мислення та здатності в застосуванні різнопланових підходів до його виявлення та переслідування. Зрозуміло, що підґрунтям ефективної боротьби та протидії злочинному явищу кібервідмивання коштів є сильна законодавча та регуляторна база. Уряди та міжнародні організації повинні бути зацікавлені у співпраці в сфері розбудови дієвих правил боротьби з відмиванням коштів з огляду на сучасні кіберзагрози [8].

За наявності правового регулювання проблеми кібервідмивання, наступним важливим елементом буде використання розширених аналітичних даних. Використання великих даних (big data) та машинного навчання можуть стати у нагоді при виявленні підозрілих операцій або схем, які б за звичайної діяльності залишилися непоміченими.

Окрім вищевказаного, не останню роль відіграє підвищення публічної обізнаності. Люди потребують знань та інформації в частині визначення проблеми кібервідмивання та способів і засобів протидії або убезпечення. Інформування про ризики кібервідмивання або методи виявлення потенційних схем стануть у нагоді не лише компаніям, але і простим громадянам, які несвідомо можуть бути використаними у схемах кібервідмивання [12].

Ну і звісно, ключовим елементом ефективної протидії будь-яким злочинам є наявність міжвідомчої взаємодії та координації. Ефективні контрзаходи вимагають скоординованих дій регуляторних органів, правоохоронних органів та фінансових установ.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Цифровий ландшафт створив нові канали для відмивання коштів та створив численні перепони на шляху протидії цим злочинам, іноді зробивши їх майже непереборними. Кібервідмивання це виняткове мистецтво відмивання коштів, яке використовує найбільший ресурс мережі Інтернет для переміщення незаконних коштів через кордони.

Сучасні технологічні рішення можуть допомогти у боротьбі з кібервідмиванням та частково зрушити важіль на користь доброї справи у цій безкінечній битві. Використовуючи допомогу алгоритмів машинного навчання та потужну аналітику, компанії приватного сектору та державні установи зможуть не лише підтвердити свій статус відповідності стандартам, передбаченим законодавством або правилами, але й показати ефективну боротьбу і протидію відмиванню коштів у найбільш широкому значенні. Відповідно, важливим елементом є обізнаність державного і приватного секторів щодо сучасних методів кібервідмивання. Це колективна боротьба, яка вимагає постійної уваги, сучасних нормативних актів та використання передових технологій для ефективної мінімізації ризику кібервідмивання. Боротьба з кібервідмиванням та кіберзлочинами вимагає постійного співробітництва та вдосконалення для того щоб встигати за злочинними геніями кіберпростору.

Подальші дослідження варто зосередити на створенні ефективних методів і алгоритмів, впровадження їх у спеціалізовані системи моніторингу кіберпростору як опорних точок протидії кібервідмиванню незаконних фінансових активів і проактивній протидії проявам кібертероризму як складової частини при побудові оптимізованих по вартості і функціоналу систем кібербезпеки інформаційних ресурсів.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Cyber-Laundering and Cyberterrorism - Sanction Scanner*. (n.d.). Sanction Scanner: Anti-Money Laundering Solutions - Sanction Scanner. https://sanctionscanner.com/blog/cyber-laundering-and-cyberterrorism-494/
2. *Internet history, design, advanced use, help, security, important features... | LivingInternet*. (n.d.). LivingInternet. https://www.livinginternet.com/
3. *Digital 2023: Global Overview Report — DataReportal – Global Digital Insights*. (n.d.). DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2023-global-overview-report?trk=article-ssr-frontend-pulse_little-text-block
4. *About YouTube - YouTube*. (n.d.). About YouTube - YouTube. https://about.youtube/
5. *Internet Borders: Where the Information Stops - ANTHONY HUGHES MEDIA*. (n.d.). ANTHONY HUGHES MEDIA. https://anthonyhughesmedia.com/internet-borders-where-the-information-stops/
6. *How are Cybercrime and Money Laundering Related?* (n.d.). ComplyAdvantage. https://complyadvantage.com/insights/cybercrime-money-laundering/
7. *Cyber Money Laundering: An In-Depth Analysis*. (n.d.). Anti-Fraud and Anti-Money Laundering (AML) Solutions | Tookitaki. https://www.tookitaki.com/blog/cyber-laundering-cyberterrorism/
8. Handa, R. K., & Ansari, R. (2022). Cyber-laundering: An Emerging Challenge for Law Enforcement. *Journal of Victimology and Victim Justice, 5(1).* https://doi.org/10.1177/25166069221115901
9. *Cyber solidarity act: member states agree common position to strengthen cyber security capacities in the EU*. (2023). https://www.consilium.europa.eu/en/press/press-releases/2023/12/20/cyber-solidarity-act-member-states-agree-common-position-to-strengthen-cyber-security-capacities-in-the-eu/

10. *Regulation - 2022/2065 - EN - DSA - EUR-Lex.* (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/eli/reg/2022/2065/oj/
11. Гуржій, С. Г., Клюшке, С. М., & Борсуковська, В. Ю. (2008). *Протидія легалізації злочинних доходів і фінансуванню тероризму : навч. посіб.* Такі справи.
12. Борсуковський, Ю. В., Борсуковська, В. Ю., Бурячок, В. Л., & Складанний, П. М. (2018). Прикладні аспекти розробки політики категорування інформації з обмеженим доступом. *Системи обробки інформації, 2(153),* 117–126. https://doi.org/10.30748/soi.2018.153.15

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023

**Victoria Borsukovska**
AML Officer
PJSC Kyivstar, Kyiv, Ukraine
ORCID ID: 0000-0002-4929-6987
*v.barsik@gmail.com*

**Yurii Borsukovskyi**
Associate Professor Information and Cyber Security Department
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0003-1973-2386
*Y.Borsukovskyi@duikt.edu.ua*

# FINANCIAL CRIMES IN CYBER SPACE: RISKS AND THREATS OF LEGALIZATION OF ILLEGAL FINANCIAL ASSETS

**Abstract.** The current Article covers the issues of counteraction to financial crimes in cyberspace. Cyberlaundering pose the significant threat to the world financial system as it assists criminals in concealing and further use of illicit assets. It also poses the challenge for law enforcement agencies which should adjust its methods in order not to fall behind the developing digital landscape. The Article considers the issue of modern technologies use for conduction of cybercrimes aimed at breach, destruction or creation threats to critical infrastructure and/or spreading of fears or panics with the ultimate goal in causing physical or economic damage to society or its population. The Article provides analysis of interaction between legalization of financial assets in cyberspace and cyberterrorism. It notes that the new type of terrorism uses the interconnectivity and vulnerability of digital systems and networks of modern society to reach it criminal goals. During last decade the cyberterrorism threat became more urgent problem for governments as well for businesses. Considering technologies continue to develop and more and more resources of critical infrastructure are connected to the world digital network the probability of cyberattacks to damage and failures became seriously real then ever before. The use of digital currencies significantly exacerbates and deepens these problems. The creation of digital currencies at the state level ensures direct trade procedures with countries which accept such payments without any converting at commonly used world currencies. It assists in concealment of source of financial transactions. Respectfully the world faces with issues for development of methods and algorithms of detection and proactive counteraction to financial crimes at cyberspace as an integral part of overall cybersecurity of information resources.

**Keywords:** cyber laundering; predicate crime; cyber terrorism; cyber-attack; cyber security.

## REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *Cyber-Laundering and Cyberterrorism - Sanction Scanner*. (n.d.). Sanction Scanner: Anti-Money Laundering Solutions - Sanction Scanner. https://sanctionscanner.com/blog/cyber-laundering-and-cyberterrorism-494/
2. *Internet history, design, advanced use, help, security, important features... | LivingInternet*. (n.d.). LivingInternet. https://www.livinginternet.com/
3. *Digital 2023: Global Overview Report — DataReportal – Global Digital Insights*. (n.d.). DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2023-global-overview-report?trk=article-ssr-frontend-pulse_little-text-block
4. *About YouTube - YouTube*. (n.d.). About YouTube - YouTube. https://about.youtube/
5. *Internet Borders: Where the Information Stops - ANTHONY HUGHES MEDIA*. (n.d.). ANTHONY HUGHES MEDIA. https://anthonyhughesmedia.com/internet-borders-where-the-information-stops/
6. *How are Cybercrime and Money Laundering Related?* (n.d.). ComplyAdvantage. https://complyadvantage.com/insights/cybercrime-money-laundering/
7. *Cyber Money Laundering: An In-Depth Analysis*. (n.d.). Anti-Fraud and Anti-Money Laundering (AML) Solutions | Tookitaki. https://www.tookitaki.com/blog/cyber-laundering-cyberterrorism/

8. Handa, R. K., & Ansari, R. (2022). Cyber-laundering: An Emerging Challenge for Law Enforcement. *Journal of Victimology and Victim Justice*, *5(1).* https://doi.org/10.1177/25166069221115901
9. *Cyber solidarity act: member states agree common position to strengthen cyber security capacities in the EU*. (2023). https://www.consilium.europa.eu/en/press/press-releases/2023/12/20/cyber-solidarity-act-member-states-agree-common-position-to-strengthen-cyber-security-capacities-in-the-eu/
10. *Regulation - 2022/2065 - EN - DSA - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/eli/reg/2022/2065/oj/
11. Gurzhii, S. G., Klyushke, S. M., Borsukovska, V. Y. (2008). *Combating the legalization of criminal income and the financing of terrorism: training.* Such cases.
12. Borsukovskyi, Y. V., Borsukovska, V. Y., Buryachok, V. L., Skladanniy, P. M. (2018). Applied aspects of policy development for categorization of information with limited access. *Information processing systems, 2(153),* 117–126. https://doi.org/10.30748/soi.2018.153.15