УДК 343.9
DOI https://doi.org/10.32782/2307-1745.2025.76.9

Кардашевський Ю. Р.,
доктор філософії у галузі права,
керівник відділу внутрішнього контролю
Національного агентства з питань запобігання корупції

Панченко Є. В.,
перший заступник начальника
Департаменту міжнародного поліцейського співробітництва
Національної поліції України

ІНСТРУМЕНТИ ТА РИЗИКИ ФІНАНСОВИХ ПОТОКІВ В КРИМІНАЛЬНОМУ КІБЕРСЕРЕДОВИЩІ

Анотація. У статті розкрито актуальні аспекти фінансової активності кіберзлочинців у сучасному цифровому середовищі, що набуває особливої загрози для національної безпеки, особливо в умовах воєнного стану в Україні. Автор системно аналізує механізми, за допомогою яких кіберзлочинці здійснюють незаконну фінансову діяльність, зокрема через використання криптовалют, електронних грошей, банківських переказів і схем із залученням «грошових мулів». Дослідження ґрунтується на ризик-орієнтованому підході та експертних оцінках кіберполіції щодо загроз, пов'язаних із шахрайством з платежами, фінансуванням тероризму, відмиванням коштів і незаконним обігом цифрових активів.

Акцентовано увагу на найбільш поширених формах фінансового шахрайства, таких як фішинг, вимагання, скімінг, фейкові благодійні кампанії. Стаття містить детальну кількісну характеристику фінансових операцій між злочинцями та від жертв до злочинців, з урахуванням динаміки їх поширення до та після війни. Особливу увагу приділено використанню криптовалют (Bitcoin, Ethereum, USDT), систем електронних платежів (EasyPay, PayPal, Webmoney) та специфіці їх застосування у злочинних схемах. Автор зазначає, що платежі у криптовалюті все частіше використовуються у darkweb-середовищі, зокрема в атаках типу ransomware або купівлі нелегальних послуг. Встановлено, що найвищим рівнем ризику характеризуються шахрайство з платежами (67,1%), грошові мули (60,9%) і банківські перекази. Здійснено порівняльний аналіз сучасного та прогнозованого рівня загроз, що дозволяє сформулювати висновки щодо збереження високих ризиків та необхідності комплексної реакції.

Зроблено висновок про необхідність комплексної протидії фінансовій активності кіберзлочинців шляхом впровадження технологій моніторингу, посилення міжнародної координації та підвищення цифрової грамотності. Стаття становить інтерес для фахівців у сфері кібербезпеки, фінансового моніторингу та правоохоронної діяльності.

Ключові слова: кіберзлочинність, кіберпростір, шахрайство з платежами, електронні гроші, криптовалюта, грошові мули.

Постановка проблеми. Кримінальні фінанси кіберпростору у сучасному світі набувають критичних масштабів, впливаючи як на національну, так і на глобальну безпеку. Кіберзлочинці використовують складні схеми для легалізації коштів, отриманих незаконним шляхом, зокрема через фішинг, шахрайство, програми-вимагачі та крадіжки персональних даних. Кіберпростір стає основною платформою для організації таких операцій, що сприяє приховуванню джерел доходу, обхідній взаємодії з фінансовими регуляторами та уникненню правового переслідування.

Основною проблемою є те, що кіберзлочинці активно використовують криптовалюту, яка забезпечує анонімність транзакцій і значно ускладнює їхнє відстеження. Bitcoin, Ethereum та інші цифрові активи все частіше застосовуються для проведення платежів у «тіньовому» кіберсередовищі. Ця тенденція підкріплюється розвитком децентралізованих фінансів, які дозволяють швидко переміщати кошти без необхідності залучення традиційних банківських систем.

В умовах війни в Україні проблема кіберзлочинності й фінансування злочинної діяльності набуває особливого значення. Кіберзлочинці спрямовують свої зусилля не лише на економічні шахрайства, але й на фінансування терористичних операцій, поширення пропаганди та підривну діяльність. Водночас, гуманітарні та благодійні ініціативи стають мішенню для шахраїв, які створюють фейкові кампанії для збору коштів.

У світі спостерігається тенденція до посилення заходів боротьби з фінансовою активністю кіберзлочинців. Запроваджуються нові регуляторні ініціативи, спрямовані на моніторинг криптовалютних транзакцій і посилення контролю за децентралізованими платформами. Міжнародні організації, такі як FATF (Financial Action Task Force), активно працюють над удосконаленням стандартів для запобігання відмиванню коштів та фінансуванню тероризму. Водночас, співпраця між державами залишається викликом, оскільки кіберзлочинність не має кордонів, а швидкість розвитку технологій випереджає традиційні інструменти правоохоронних органів.

Таким чином, фінансова активність кіберзлочинців у кіберпросторі потребує комплексного підходу до вирішення. Це включає посилення міжнародної координації, впровадження інноваційних технологій для моніторингу транзакцій, а також підвищення кіберобізнаності населення. Для України ця проблема є вкрай актуальною, оскільки боротьба з кіберзлочинністю є важливою складовою захисту національної безпеки під час війни.

У дослідженнях багатьох відомих вітчизняних дослідників, значна увага приділяється різним проблемам, пов'язаним з розробкою напрямів щодо кібербезпеки, зокрема протидії кіберзлочинності: Бєлякова К.І. [1], Бутузова В.М. [2], Веселової Л.Ю. [3], Гуцалюка М.В. [4; 5], Довганя О.Д. [6], Казмірчук С. [7], Корченка О.Г. [7], Марущака А.І. [8], Гавловського В.Д. [9; 10], Хахановського В.Г. [10], Шеломенцева В.П. [11] та інших.

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 висказувалися щодо методології Європолу IOCTA [12], яка є головним стратегічним продуктом Європолу, що забезпечує орієнтовану на правоохоронні органи оцінку нових загроз і ключових подій у сфері кіберзлочинності.

Значну увагу цим питанням приділяли у своїх роботах науковці та фахівці в зарубіжних виданнях. Зокрема, дослідження [13] фокусується на аналізі платежів, пов'язаних із програмами-вимагачами, у біткоїн-екосистемі. Автори використовують методи блокчейн-аналізу для відстеження руху коштів та ідентифікації ключових гравців у цих схемах. У статті [14] представлено типологію взаємодії між кіберзлочинністю та криптовалютами. Автори класифікують різні способи використання цифрових валют у злочинних цілях та пропонують рекомендації для правоохоронних органів щодо протидії таким практикам. У дослідженні інших авторів [15] здійснюється аналіз впливу анонімності та використання криптовалют на поведінку осіб в онлайн-середовищі. Автори аналізують, як ці фактори можуть сприяти кіберзлочинності та які заходи можуть бути ефективними для її запобігання.

Водночас відчизняними вченими активно використовується ризик-орієнтований підхід щодо аналізу проблем у сфері безпеки та кібербезпеки [16–20].

Метою статті є дослідження активності злочинців у кіберпросторі, виклики щодо використання альтернативних фінансових інструментів та оцінка відповідних ризиків.

Виклад основного матеріалу. Значна частина кіберзлочинів вчиняється фінансово мотивованими злочинцями. Таким злочинцям, які займаються торгівлею на кримінальних ринках або вимаганням грошей від своїх жертв, потрібні певні кошти чи інші фінансові інструменти для здійснення та отримання прибутку від своєї діяльності. У «реальних» злочинах це, швидше за все, була б готівка в місцевій або вільно конвертованій валюті, але кіберзлочинцям, які працюють у цифровому світі, потрібне цифрове рішення.

Фінансова активність, перш за все, пов'язується з отриманням швидкого прибутку і мінімізацією ризиків для самих кіберзлочинців, та набуває самих різних форм:

– фінансові шахрайства: *використання фішингу, скіммінгу, та інших методів для отримання доступу до банківських рахунків та кредитних карток*;

– фінансові транзакції від жертв до злочинців та між злочинцями: *використання новітніх банківських послуг та сучасних фінансових інструментів*.

Експертним середовищем кіберполіції [20] було оцінено окремі індикатори як загрози, що характеризують фінансову активність кіберзлочинців (*табл. 1*).

За сучасного стану найбільшим поширенням характеризуються загрози шахрайства з платежами (67,10%), водночас є значною фінансова активність, пов'язана з платежами від жертв до злочинців (60,90%). Такий тренд зберігався упродовж останніх років та є характерним також у післявоєнний період, зокрема: значним рівнем ризику у майбутньому характеризується шахрайство з платежами (45,37%) та фінансова активність, пов'язана з платежами від жертв до злочинців (44,42%).

Серед фінансових інструментів, що використовують *жертви шахрайства*, найбільшим поширенням характеризуються традиційні – банківські перекази (66,0%) та використання платіжних карток – 64,3%), тренд високого рівня за якими, зберігається упродовж останніх років та характеризується найвищим рівнем ризику у післявоєнний період (*табл. 2*).

Водночас, високим рівнем використання також визначаються платежі від жертв злочинів, що здійснюються шляхом купівлі предметів та речей (50,9%) та з використанням криптовалют (48,6%). При цьому, значним поширенням характеризується шахрайське поповнення мобільного рахунку (43,7%) та використання електронних грошей (42,6%).

Співвідношення активності використання різних фінансових інструментів жертвами шахрайства, залишається сталим як упродовж останніх років, так і відповідно таким самим чином характеризується тренд у післявоєнний період.

Використовуючи *криптовалюти* у якості платежів від жертв злочинів, найбільша активність стосується: Bitcoin (53,7%), USDT (46,9%) та Ethereum (40,6%) (*табл. 3*).

Bitcoin найпопулярніша валюта для здійснення розрахунків між злочинцями, наприклад, під час придбання або оренди ін-

Таблиця 1

Фінансова активність кіберзлочинців

ВИДИ ФІНАНСОВОЇ АКТИВНОСТІ КІБЕРЗЛОЧИНЦІВ	**Оцінка сучасного поширення**	**%**	Масштаби збільшились	Масштаби не змінились	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

Таблиця 2

Рівень ризиків фінансової активності за платежами від жертв до злочинців

ПЛАТЕЖІ ВІД ЖЕРТВ ДО ЗЛОЧИНЦІВ	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
5.1.Банківські перекази		66,00				43,70
5.2.Платіжна картка		64,30				43,91
5.3.Шляхом поповнення мобільного рахунку		43,70				38,18
5.4.Шляхом покупки якогось предмету, речі		50,90				40,54
5.5.Системи оплати ваучерами (наприклад, paysafecard)		27,40				33,38
5.6.Використання електронних грошей		42,60				39,74
5.7.Використання криптовалюти		48,60				41,35

Таблиця 3

Рівень ризиків платежів від жертв до злочинців за видами криптовалют

ПЛАТЕЖІ ВІД ЖЕРТВ ДО ЗЛОЧИНЦІВ: криптовалюта	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
7.1.Bitcoin		53,70				40,05
7.2.Ethereum		40,60				37,44
7.3.Ripple		26,00				32,63
7.4.Monero		28,00				33,38
7.5.BNB		29,40				32,09
7.6.USDT		46,90				38,12
7.7.USDC		32,00				33,50
7.8.Zcash		23,40				31,76
7.9.Dash		25,10				31,89
7.10.Litecoin		30,60				32,59

струментів або послуг для вчинення кіберзлочинів у цифровому підпіллі. Це єдина валюта, яку приймають в більшості магазинів у Darknet та автоматизованих магазинів карток, і валюта, яку вимагають як викуп у майже у всіх сьогоднішніх атаках з використанням програм-вимагачів або DoS-атаках.

Незважаючи на те, що використання Bitcoin у злочинних цілях залишається ключовим фактором, що сприяє злочинній поведінці в мережі Інтернет, у цифровому підпіллі зростає активність інших криптовалют (23,4%–29,4%).

При використанні *електронних грошей*, у якості платежів від жертв злочинів до злочинців, найчастіше використовуються системи: EasyPay (47,1%), PayPal (42,0%), а також Webmoney (35,4%) та Qiwi (32,6%) (*табл. 4*).

У післявоєнний період залишається переважно без змін співвідношення щодо використання найбільш поширених систем електронних грошей для здійснення платежів від жертв злочинів до злочинців, а найвищий рівень ризику передбачається щодо: EasyPay (37,88%), PayPal (35,73%), Webmoney (34,27%).

Інші системи електронних грошей також використовуються для платежів від жертв злочинів до злочинців, але відносно зазначених вище систем цей рівень є дещо нижчим (25,4%–28,6%).

Значною у кіберпросторі є фінансова активність, що пов'язана з *платежами між злочинцями*. Серед фінансових інструментів, що використовуються для здійснення платежів між злочинцями, найбільшим поширенням характеризуються – грошові мули (60,9%), використання банківських карток (60,9%) та банківські перекази (56,9%). Водночас, упродовж останніх років тренд високого рівня зберігався більше за грошовими мулами та характеризується найвищим рівнем ризику у післявоєнний період (*табл. 5*).

Багато кіберзалежних злочинів в певний момент породжують фіатну валюту з регульованим фінансовим сектором, незалежно від того, чи вона отримана із скомпрометованого банківського рахунка жертви чи з банкомату, зараженого шкідливим програмним забезпеченням. Доступ до цих коштів часто становить значно більший ризик, ніж дії, спрямовані на те, щоб перевести їх під контроль злочинців. Саме тут з'являється потреба в послугах третьої сторони – «грошових мулів».

Тренд у майбутньому щодо традиційних банківських фінансових послуг хоча і є відносно меншим за рівнем ризику, у порівнянні з використанням грошових мулів, все ж у пер-

Таблиця 4

Платежі від жертв до злочинців за видами електронних грошей

ПЛАТЕЖІ ВІД ЖЕРТВ ДО ЗЛОЧИНЦІВ: електронні гроші	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
6.1.Webmoney		35,40				34,27
6.2.PerfectMoney		28,60				33,46
6.3.Юmoney		25,40				32,06
6.4.Qiwi		32,60				33,34
6.5.PayPal		42,00				35,73
6.6.Advanced Cash		26,60				32,47
6.7.Payeer		27,70				33,16
6.8.Skrill		26,30				32,44
6.9.EasyPay		47,10				37,88

Таблиця 5

Рівень ризиків фінансової активності за платежами між злочинцями

ПЛАТЕЖІ МІЖ ЗЛОЧИНЦЯМИ	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
4.1. Грошові мули (дропи)		60,9				45,62
4.2. Банківські перекази		56,9				42,14
4.3. Банківська картка		60,6				43,08
4.4. Системи оплати ваучерами (наприклад, paysafecard)		31,4				34,92

спективі оцінюється експертним середовище на рівні вищому 40% і зниження рівня ризику є лише відносним, у порівнянні з використанням грошових мулів.

Використовуючи *криптовалюти* у якості платежів між злочинцями найбільш поширеними також є Bitcoin (54,9%), USDT (45,4%) та Ethereum (43,4%) (*табл. 6*).

Інші види криптовалют також використовуються для платежів між злочинцями, але відносно зазначених вище видів цей рівень є дещо нижчим (27,7%–34,6%).

Такий же тренд за видами криптовалют, що використовуються для здійснення платежів між злочинцями, зберігався упродовж останніх років. Більше того, відзначається певне

Таблиця 6

Рівень ризиків платежів між злочинцями за видами криптовалют

ПЛАТЕЖІ МІЖ ЗЛОЧИНЦЯМИ: криптовалюти	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
4.14. Bitcoin		54,90				41,35
4.15. Ethereum		43,40				38,12
4.16. Ripple		29,70				33,52
4.17. Monero		30,90				34,59
4.18. BNB		33,40				33,26
4.19. USDT		45,40				39,14
4.20. USDC		34,60				34,86
4.21. Zcash		28,00				32,72
4.22. Dash		27,70				32,62
4.23. Litecoin		32,00				33,46

збільшення масштабів використання Bitcoin, USDT та Ethereum навіть у період воєнного стану.

Рівень ризиків у післявоєнний період характеризується збереженням співвідношення між активністю використання різних видів криптовалют та підвищенням у платежах між злочинцями USDC (33,5%) та Monero (33,38%).

При використанні *електронних грошей*, у якості платежів між злочинцями, найчастіше використовуються системи: EasyPay (46,6%), PayPal (42,6%), а також Webmoney (34,0%), Qiwi (32,0%) та PerfectMoney (31,4%) (*табл. 7*). Інші системи електронних грошей також використовуються для платежів між злочинцями, але відносно зазначених вище систем цей рівень є дещо нижчим (26,3%–30,3%).

Такий же тренд за видами систем електронних грошей, що використовуються для здійснення платежів між злочинцями, з перевагою EasyPay та PayPal, зберігався упродовж останніх років.

Водночас, у післявоєнний період щодо використання окремих найбільш поширених систем електронних грошей для здійснення платежів між злочинцями, експертним середовищем передбачається зниження рівня ризику їх використання, у порівнянні з іншими системами, хоча все ще відносно більшим рівнем ризику: EasyPay (37,94%), PayPal (36,99%).

Висновки. Фінансова активність кіберзлочинців є ключовим компонентом сучасної кіберзлочинності. Шахрайство з платежами є найбільш поширеною загрозою у сфері кіберзлочин-

Таблиця 7

Рівень ризиків платежів між злочинцями за видами електронних грошей

ПЛАТЕЖІ МІЖ ЗЛОЧИНЦЯМИ: електронні гроші	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
4.5. Webmoney		34,00				35,14
4.6. PerfectMoney		31,40				34,32
4.7. ЮMoney		28,90				33,08
4.8. Qiwi		32,00				34,81
4.9. PayPal		42,60				36,99
4.10. Advanced Cash		26,30				33,05
4.11. Payeer		30,30				33,62
4.12. Skrill		26,60				32,33
4.13. EasyPay		46,60				37,94

ності, складаючи 67,10% усіх випадків. Воно характеризується високим рівнем ризику і залишається важливою проблемою як до, так і після війни. Фінансова активність, пов'язана з прямими платежами від жертв до злочинців, також є значною (60,90%).

Традиційні фінансові інструменти, такі як банківські перекази (66,0%) і платіжні картки (64,3%), залишаються основними засобами, які використовують жертви шахрайства. Їх використання є стабільним і характеризується високим рівнем ризику у післявоєнний період.

Криптовалюти також активно використовуються в злочинних схемах. Найчастіше використовуються Bitcoin (53,7%), USDT (46,9%), Ethereum (40,6%), а також інші види криптовалют, що займають значну частку (23,4%–29,4%). У післявоєнний період очікується зниження ризику для Bitcoin, USDT, Ethereum, але підвищення ризику для інших криптовалют.

Електронні гроші є значним компонентом у платежах від жертв злочинів, особливо такі системи, як EasyPay (47,1%) і PayPal (42,0%). Зазначається прогноз зниження рівня ризику для найпоширеніших систем електронних грошей у майбутньому, але підвищення для інших систем.

Література:

1. Бєляков К.І. Інформація в праві: теорія і практика: монографія. Київ: Видавництво «КВІЦ», 2006. 116 с.
2. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія. Київ: КИТ, 2010. 408 с.
3. Користін О.Є., Веселова Л.Ю. Ризикорієнтованість кібербезпеки. Наука і правоохоронна. 2021. № 3. С. 16–23.
4. Гуцалюк М.В. Сучасні тенденції організованої кіберзлочинності. Інформація і право. 2019. № 1(28). С. 118–128.
5. Гуцалюк М.В., Хахановський В.Г. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. Криміналістичний вісник. 2020. № 31(1). С. 13–19. https://doi.org/10.37025/1992-4437/2019-31-1-13.
6. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кібезахисту: монографія. Київ: Видавничий дім «АртЕк», 2017. 107 с.
7. Корченко О., Казмірчук С., Ахметов Б. Прикладні системи оцінювання ризиків інформаційної безпеки: монографія, Київ: ЦП Компринт, 2017. 435 с.
8. Марущак А.І. Інформаційні ресурси держави: зміст та проблема захисту. Правова інформатика. 2009. № 1(21). С. 65–71.
9. 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.
10. Хахановський В.Г., Гавловський В.Д. Тлумачення та класифікація кримінальних правопорушень як кіберзлочинів. Інформація і право. 2020. № 2(33). С. 99–110.
11. Шеломенцев В.П. Організована кіберзлочинність: до визначення поняття. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2009. Вип. 21. С. 314–322.
12. Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021. Publications Office of the European Union. Luxembourg. 2021.
13. Masarah Paquet-Clouston, Bernhard Haslhofer, Benoît Dupont, Ransomware payments in the Bitcoin ecosystem, Journal of Cybersecurity, Volume 5, Issue 1, 2019, tyz003, https://doi.org/10.1093/cybsec/tyz003
14. Samira Ibrahim, et. al. «Cybercrimeand Cryptocurrency."American Journal of EngineeringResearch (AJER), vol. 10(12), 2021, pp. 103–106.

15. Bray, Jesse D., «Anonymity, Cybercrime, and the Connection to Cryptocurrency» (2016). Online Theses and Dissertations. 344.
16. Kovalchuk T.I., Korystin O. Y., Sviridyuk N. P. Hybrid threats in the civil security sector in Ukraine. Problems of Legality. 2019. № 147. 163–175. DOI: https://doi.org/10.21564/2414-990x.147.180550
17. 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). Series: Advances in Economics, Business and Management Research. 27 August 2021. Vol. 188. Pp. 65–69. DOI: 10.2991/AEBMR.K.210826.012
18. Користін О.Є., Цюприк І.В., Свиридюк Н.П., Прокоф'єфа-Янченко 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)
19. Користін О.Є., Свиридюк Н.П. Оцінювання загроз у сфері лісового господарства України. Наука і правоохорона. 2023. № 1. С. 145–153. DOI (Issue): https: //doi.org/10.36486/np.2023.1(59)
20. Користін О.Є., Демедюк С.В., Панченко Є.В., Користін О.О. Національні реалії аналізу кіберзлочинності за методологією Європолу ІОСТА. Південноукраїнський правничий часопис. № 3. 2023. С. 44–46. DOI https://doi.org/10.32850/sulj.2023.3.10

Kardashevskyy Yu. Panchenko Ye. Tools and risks of financial flows in the criminal cyber environment

Summary. The article explores current aspects of cybercriminals' financial activity in the modern digital environment, which poses an increasing threat to national security, particularly under martial law in Ukraine. The author systematically analyzes the mechanisms through which cybercriminals conduct illicit financial operations, including the use of cryptocurrencies, electronic money, bank transfers, and schemes involving «money mules.» The research is based on a risk-oriented approach and expert assessments by the cyber police regarding threats related to payment fraud, terrorism financing, money laundering, and the illegal circulation of digital assets.

Particular attention is paid to the most widespread forms of financial fraud, such as phishing, extortion, skimming, and fake charitable campaigns. The article provides a detailed quantitative assessment of financial operations both between criminals and from victims to criminals, taking into account trends observed before and after the onset of the war. A special focus is given to the use of cryptocurrencies (Bitcoin, Ethereum, USDT), electronic payment systems (EasyPay, PayPal, Webmoney), and their specific application in criminal schemes. The author notes that cryptocurrency payments are increasingly used in dark web environments, particularly in ransomware attacks or the purchase of illicit services. It is established that the highest levels of risk are associated with payment fraud (67.1%), money mules (60.9%), and bank transfers.

A comparative analysis of current and projected threat levels is carried out, allowing for conclusions regarding the persistence of high risks and the need for a comprehensive response. The article concludes with the recommendation to counteract the financial activity of cybercriminals through the implementation of transaction monitoring technologies, enhancement of international coordination, and improvement of digital literacy. The study is of interest to professionals in the fields of cybersecurity, financial monitoring, and law enforcement.

Key words: cybercrime, cyberspace, payment fraud, electronic money, cryptocurrency, money mules.

Дата надходження статті: 11.08.2025
Дата прийняття статті: 01.09.2025
Опубліковано: 30.09.2025