

Панченко Євгеній Вікторович,
начальник 4-го управління (оперативно-аналітичного забезпечення та аналізу відкритих джерел) Департаменту кіберполіції Національної поліції України

КРИПТОВАЛЮТИ Й ЕЛЕКТРОННІ ГРОШІ ЯК ІНСТРУМЕНТИ ФІНАНСОВОЇ АКТИВНОСТІ КІБЕРЗЛОЧИНЦІВ

Експертним середовищем кіберполіції було оцінено окремі загрози, що характеризують фінансову активність кіберзлочинців.

Використовуючи криптовалюти у якості платежів від жертв злочинів, найбільша активність стосується: Bitcoin (53,7 %), USDT (46,9 %) та Ethereum (40,6 %) (табл. 1).

Таблиця 1

Рівень ризиків платежів від жертв до злочинців за видами криптовалют

ПЛАТЕЖІ ВІД ЖЕРТВ ДО ЗЛОЧИНЦІВ: криптовалюта	Оцінка сучасного поширення	%	Масштаби збільшилися	Масштаби не змінилися	Масштаби зменшилися	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

Bitcoin найпопулярніша валюта для здійснення розрахунків між злочинцями, наприклад, під час придбання або оренди інструментів 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 сьогодишніх 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.

Monero – з'явилася у 2014 році. Більша частина зростаючої популярності Monero пов'язана з додатковими функціями безпеки та конфіденційності, які вона пропонує; транзакції не можуть бути віднесені до конкретного користувача/адреси, всі монети, що використовуються в транзакції, «приховані» за замовчуванням, а історія транзакцій є приватними. Monero зараз приймають у низці ринків в Darknet, а в 2017 році з'явилася перша програма вимагач – Kirk, в якій викуп потрібно було сплатити у криптовалюті Monero.

Ethereum – «smart-контракти» Ethereum можуть стати інструментом для бізнес-моделі «злочин як послуга». Поки що цього не сталося, але принаймні певні ринки в Darknet приймають Ethereum для здійснення платежів і покупок.

Zcash – це ще одна криптовалюта, яка забезпечує підвищений рівень конфіденційності для своїх користувачів, приховуючи як одержувача транзакції, так і суму транзакції.

Інші види криптовалют також використовуються для здійснення платежів від жертв злочинів до злочинців, але відносно зазначених вище видів цей рівень є дещо нижчим (23,4 %–29,4 %).

Упродовж останніх років тренд за видами криптовалют, що використовуються для здійснення платежів від жертв злочинів до злочинців, залишається без особливих змін.

У післявоєнний період залишається переважно без змін співвідношення щодо використання найбільш поширених видів криптовалют для здійснення платежів від жертв злочинів до злочинців, а найвищий рівень ризику передбачається щодо Bitcoin (40,05 %), USDT (38,12 %) та Ethereum (37,44 %).

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. 2).

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 %).

Таблиця 2

Платежі від жертв до злочинців за видами електронних грошей

ПЛАТЕЖІ ВІД ЖЕРТВ ДО ЗЛОЧИНЦІВ: електронні гроші	Оцінка сучасного поширення	%	Масштаби збільшилися	Масштаби не змінювалися	Масштаби зменшилися	Ризик після війни, %
6.1.Webmoney		35,40				34,27
6.2.PerfectMoney		28,60				33,46
6.3.Yomoney		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

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

Використовуючи криптовалюти у якості платежів між злочинцями найбільш поширеними також є Bitcoin (54,9 %), USDT (45,4 %) та Ethereum (43,4 %) (табл. 3). Інші види криптовалют також використовуються для платежів між злочинцями, але відносно зазначених вище видів цей рівень є дещо нижчим (27,7 %–34,6 %).

Таблиця 3

Рівень ризиків платежів між злочинцями за видами криптовалют

ПЛАТЕЖІ МІЖ ЗЛОЧИНЦЯМИ: криптовалюти	Оцінка сучасного поширення	%	Масштаби збільшилися	Масштаби не змінювалися	Масштаби зменшилися	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

Такий же тренд за видами криптовалют, що використовуються для здійснення платежів між злочинцями, зберігався упродовж останніх років. Більше того, відзначається певне 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. 4). 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.

Таблиця 4

Рівень ризиків платежів між злочинцями за видами електронних грошей

ПЛАТЕЖІ МІЖ ЗЛОЧИНЦЯМИ: електронні гроші	Оцінка сучасного поширення	%	Масштаби збільшилися	Масштаби не змінилися	Масштаби зменшилися	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

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 %).

Таким чином, криптовалюти 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.

Петров Вадим Амінович,

заступник начальника 1-го управління
(аналітичного) – начальник 1-го відділу
(кримінального аналізу) Департаменту
кримінального аналізу Національної
поліції України

КЛЮЧОВІ НАПРЯМИ РОЗВИТКУ ТАКТИЧНОГО КРИМІНАЛЬНОГО АНАЛІЗУ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ У 2024 РОЦІ

Департамент в своїй діяльності на постійній основі займається збором та аналізом інформації про кримінальну ситуацію, з метою забезпечення ефективного контролю та протидії злочинності.

Метод дослідження конкретної події обставин чи сукупності факторів, які призвели до кримінальної події або можуть сприяти її розвитку – називається ситуаційний аналіз.

Основні завдання ситуаційного аналізу:

– визначення контексту події: дослідження зовнішніх обставин, що могли сприяти злочину (наприклад, соціально-економічні, політичні, культурні умови);

– виявлення мотивів і причин: аналіз факторів, які призвели до злочинного діяння, включаючи психологічні, соціальні та економічні передумови;

– ідентифікація залучених осіб і груп: вивчення профілю осіб, які брали участь у події, включаючи їхню історію, можливі зв'язки, роль і мотиви;