Міністерство освіти і науки України
Сумський державний університет
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра економічної кібернетики

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

Матеріали
наукової онлайн-конференції

(Суми, 07 вересня 2023)

Суми
Сумський державний університет
2023

004.056.5:336(082)
В43

Головний редактор
доц., к.е.н., Prof., Dr. ***Койбічук Віталія***, завідувачка кафедри економічної кібернетики, Сумський державний університет
.

Затверджено Вченою Радою Сумського державного університету (протокол № 2, 14.09.2023)

S62 Виклики кібербезпеки індустрії фінансових послуг: Матеріали наукової онлайн-конференції, Суми, 07 вересня 2023. Збірник матеріалів тез наукової онлайн-конференції / за загальною редакцією доц. Койбічук В.В. – Суми : Сумський державний університет, 2023. – 183 с.

Матеріали наукової онлайн-конференції " Виклики кібербезпеки індустрії фінансових послуг" присвячені пошуку системного вирішення проблем у сфері протидії кібеззагрозам у сфері фінансових послуг, підвищенню рівня кіберзахисту об'єктів критичної інфраструктури.

Видання розраховане на науковців, викладачів, студентів вищих навчальних закладів, аспірантів, докторантів та інших зацікавлених осіб.

004.056.5:336(082)

© Сумський державний університет, 2023

ЗМІСТ

СЕКЦІЯ 1	***ЦИФРОВІ ТРАНСФОРМАЦІЇ В ЕКОНОМІЦІ***	6
Кирило Каліновський, Валерій Яценко	ЕЛЕКТРОННІ ФІНАНСОВІ ПОСЛУГИ ЯК ІНСТРУМЕНТ РОЗВИТКУ ЦИФРОВОЇ ЕКОНОМІКИ	6
Єлизавета Калюсенко	ЦИФРОВІ ТРАНСФОРМАЦІЇ В ЕКОНОМІЦІ	9
Сергій Миненко, Владислава Лук'янова	АНАЛІЗ РІВНЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ УКРАЇНИ ТА КРАЇН ЄС	12
Анастасія Самойленко, Валерій Яценко	РОЗУМНІ МІСТА ТА ЇХ РОЛЬ У ЦИФРОВІЙ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ	16
Аліна Сімановська	ЦИФРОВІ ТРАНСФОРМАЦІЇ В БАНКІВСЬКІЙ СФЕРІ: ТЕНДЕНЦІЇ ТА МОЖЛИВОСТІ	19
Ігор Бараннік, Олексій Бударін	ЗРОСТАННЯ ЕКОНОМІЧНОЇ СТІЙКОСТІ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ В СУЧАСНИХ УМОВАХ ДІЯЛЬНОСТІ	22
Анастасія Кузченко, Валерій Яценко	РОЗВИТОК ФІНТЕХ-ІНДУСТРІЇ У СВІТІ: ТЕНДЕНЦІЇ ТА ВИКЛИКИ	24
Сергій Дрозд	КЛЮЧОВІ АСПЕКТИ ТА ВИКЛИКИ ЦИФРОВІ ТРАНСФОРМАЦІЇ В ЕКОНОМІЦІ	28
Сергій Миненко, Валерія Кочнєва	ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ МОНІТОРИНГУ ПУБЛІЧНИХ ЗАКУПІВЕЛЬ З МЕТОЮ ВИЯВЛЕННЯ ТА УНИКНЕННЯ КОРУПЦІЇ	32
Владислава Лук'янова, Валерій Яценко	ПЕРСПЕКТИВИ РОЗВИТКУ ЦИФРОВОЇ ЕКОНОМІКИ ТА ЇЇ ВПЛИВ НА СУСПІЛЬСТВО І ЛЮДЕЙ	35
Дмитро Діденко, Світлана Коломієць	РОЗВИТОК ЕЛЕКТРОННОЇ КОМЕРЦІЇ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ	38
Ілля Лубенець, Світлана Коломієць	ВПЛИВ ЦИФРОВОЇ ЕКОНОМІКИ НА СТАН ГРОМАДСЬКОГО ЗДОРОВ'Я НАСЕЛЕННЯ	41

СЕКЦІЯ 2	***КІБЕРЗАГРОЗИ У СФЕРІ ФІНАНСОВИХ ПОСЛУГ***	44
Vadym Dun, Serhii Mynenko	АНАЛІЗ ВПЛИВУ ВЕЛИКИХ КІБЕРІНЦИДЕНТІВ НА АКЦІЇ КОМПАНІЇ	44
Kuan Zhang	THE RISKS OF ELECTRONIC PAYMENTS IN CROSS-BORDER E-COMMERCE	48
Анна Голопьорова, Валерій Яценко	МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ КІБЕРБЕЗПЕКИ: ВИКЛИКИ ТА МОЖЛИВОСТІ	50
Олександр Воробйов, Валерій Яценко	КІБЕРБЕЗПЕКА У МЕРЕЖАХ 5G: ПРАКТИЧНІ ВИКЛИКИ ТА РИЗИКИ	53
Віталія Койбічук	КІБЕРБЕЗПЕКА БІЗНЕСУ МАЛИХ ТА СЕРЕДНІХ ПІДРПРИЄМСТВ: ДОСВІД ЄС	56
Сергій Миненко, Ксенія Могильна	ПОЗИТИВНІ Й НЕГАТИВНІ СТИМУЛИ ДО ВИКОРИСТАННЯ КРИПТОВАЛЮТ У ЕКОНОМІЧНІЙ ЗЛОЧИННОСТІ	60
Назар Фененко	ПЕРСОНАЛ КОМПАНІЇ ЯК «БРАМА» ДЛЯ КІБЕР АТАК	64
Єлизавета Литюга, Валерій Яценко	ПЕРСПЕКТИВИ РОЗВИТКУ ХАКТИВІЗМУ ТА ХАКЕРСЬКИХ АТАК В СФЕРІ ФІНАНСОВИХ ПОСЛУГ: ВИКЛИКИ ТА ШЛЯХИ ПРОТИДІЇ	67
Катерина Солярова, Ганна Яровенко	ПРОГНОЗУВАННЯ ІНФОРМАЦІЙНИХ ТРЕНДІВ КІБЕРЗЛОЧИНІВ	71
Вікторія Боженко, Олександр Роєнко	ОСОБЛИВОСТІ ДЕРЖАВНОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ ФІНАНСОВИХ УСТАНОВ У ЄВРОПЕЙСЬКОМУ СОЮЗІ	74
Вікторія Боженко, Іван Гончарук	МАСШТАБИ НЕЗАКОННОГО МАЙНІНГУ КРИПТОВАЛЮТ	77
Архипов Станіслав	КІБЕРФРОНТ У ВІЙНІ РОСІЇ ПРОТИ УКРАЇНИ	80
Ганна Яровенко	КЛЮЧОВІ АСПЕКТИ ВІДПОВІДАЛЬНОЇ ПОВЕДІНКИ СПОЖИВАЧІВ ФІНАНСОВИХ ПОСЛУГ У КІБЕРПРОСТОРІ	82

Xinxin Wang ВИКЛИКИ КІБЕРБЕЗПЕКИ, ЩО СТОЯТЬ ПЕРЕД ГАЛУЗЗЮ ФІНАНСОВИХ ПОСЛУГ 85

Олена Пахненко СОЦІО-ДЕМОГРАФІЧНІ ДЕТЕРМІНАНТИ ВРАЗЛИВОСТІ КОРИСТУВАЧІВ ФІНАНСОВИХ ПОСЛУГ ДО КІБЕРРИЗИКІВ 90

СЕКЦІЯ 3 ***ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПРОТИДІЇ КІБЕРЗАГРОЗАМ*** 93

Альона Рапута КОНВЕРГЕНЦІЯ СИСТЕМИ КІБЕРБЕЗПЕКИ ТА ПРОТИДІЇ ФІНАНСОВИМ ЗЛОЧИНАМ 93

Анастасія Савенко, Валерій Яценко КІБЕРБЕЗПЕКА В МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВАХ: РОЗРОБКА ТА ВПРОВАДЖЕННЯ СТРАТЕГІЙ ЗАХИСТУ 97

Анна Поліщук ІНВЕСТИЦІЇ В КІБЕРБЕЗПЕКУ ЯК ДРАЙВЕР РОЗВИТКУ КОМПАНІЇ 101

Діана Харченко ВАЖЛИВІСТЬ ІНВЕСТИЦІЙ У КІБЕРБЕЗПЕКУ ДЛЯ ПІДВИЩЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ КОМПАНІЙ 104

Поліна Терляківська, Валерій Яценко РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В ЦИФРОВІЙ ЕКОНОМІЦІ: ТЕХНОЛОГІЧНІ ТА ЕТИЧНІ АСПЕКТИ 107

Артем Штефан ТЕХНОЛОГІЯ БЛОКЧЕЙН ДЛЯ ПРОТИДІЇ КІБЕРЗАГРОЗАМ У СФЕРІ ФІНАНСОВИХ ПОСЛУГ 110

Катерина Славгородська, Валерій Яценко ЦИФРОВІ ІННОВАЦІЇ У ФІНАНСОВИХ ПОСЛУГАХ: НОВІ МОЖЛИВОСТІ ТА ВИКЛИКИ БЕЗПЕКИ 113

Христина Чуб, Валерій Яценко ЦИФРОВІ ТЕХНОЛОГІЇ ТА ІННОВАЦІЙНІ ПРОЦЕСИ У РОЗВИТКУ ЦИФРОВОЇ ЕКОНОМІКИ 116

Тетяна Доценко, Дарина Бережна ТЕНДЕНЦІЇ МОДЕЛЮВАННЯ DUE DILIGENCE ДЛЯ ПРОТИДІЇ ФІНАНСОВИМ КІБЕРШАХРАЙСТВАМ 120

ПОЗИТИВНІ Й НЕГАТИВНІ СТИМУЛИ ДО ВИКОРИСТАННЯ КРИПТОВАЛЮТ У ЕКОНОМІЧНІЙ ЗЛОЧИННОСТІ

POSITIVE AND NEGATIVE INCENTIVES FOR THE USE OF CRYPTOCURRENCIES IN ECONOMIC CRIME

Сергій Миненко, доктор філософії
Сумський державний університет, Україна
Ксенія Могильна, студентка
Сумський державний університет, Україна

Криптовалюти набули значного поширення протягом останніх років, проте, завдяки анонімності й децентралізації вони також стали зручним інструментом у сфері економічної злочинності. Розуміння позитивних і негативних стимулів до використання криптовалют у економічній злочинності має вирішальне значення для розробки ефективної політики та стратегій боротьби з їх незаконним використанням, тому ця тема є актуальною для наукової спільноти. Метою цієї роботи є вивчення технічних та концептуальних характеристик криптовалют, що є позитивними та негативними стимулами їх залучення до економічної злочинності.

Для усвідомлення ролі криптовалют у економічній злочинній діяльності важливо розуміти сутність поняття «криптовалюта». За визначенням (Yaga та et al., 2018) криптовалюти є цифровими активами в системі, які криптографічно надсилаються від одного користувача мережі блокчейн до іншого за допомогою цифрових підписів із парами асиметричних ключів. Основними відмінностями криптовалют від електронних національних валют є те, що їх емісують децентралізовано без участі державних установ, також криптовалюти існують виключно у цифровій формі. Ще однією відмінною рисою криптовалют є типи транзакцій, зокрема можливість переказів «від особи до особи» (або P2P) й обмінів на криптовалютних біржах. Транзакції «від особи до особи» є прямими переказами між користувачами, тобто здійснюються без залучення посередників у вигляді криптовалютних бірж або інших фінансових установ, таким чином, їх важко відслідкувати й контролювати. Обміни на криптовалютних біржах, тобто платформах, які дозволяють купувати та продавати криптовалюти, є більш публічними та захищеними за рахунок нагляду самих бірж та держави.

Очевидно, що справжній обсяг криптовалюти задіяної в економічній злочинності точно оцінити неможливо через відсутність вичерпної бази даних, яка б відстежувала всі транзакції, та анонімність багатьох переказів, що ускладнює ідентифікацію зловмисників. Однак наявні оцінки обсягів

криптовалюти пов'язаних з незаконними акаунтами здатні надати загальне уявлення про тенденції цього ринку (рис. 1). За даними дослідження Chainalysis Inc, загальна вартість криптовалюти, отримання якої було пов'язано з злочинністю, у 2022 році досягла рекордного значення 20,6 мільярдів доларів США (Grauer et al., 2023), не зважаючи на загальний спад ринку протягом року. Крім того, з рис. 1, очевидно, що протягом 2017-2022 років цей показник мав загальну тенденцію до зростання, що також свідчить про збільшення обсягів залучення крипитовалют до злочинної діяльності.

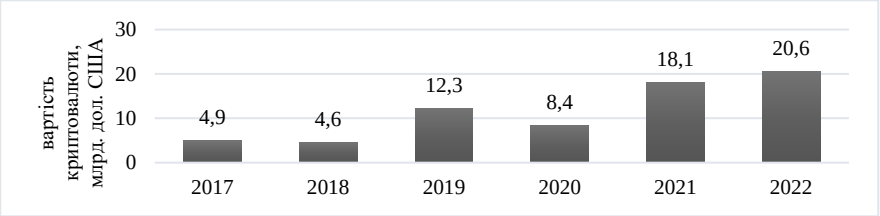

Рисунок 1. Вартість криптовалюти, отриманої незаконними акаунтами 2017-2022 років (ілюстрація створена автором на основі даних (Grauer et al., 2023)

З огляду на поширення використання криптовалют, як інструменту відмивання доходів від незаконної діяльності, шахрайства, ухилення від сплати податків, фінансування тероризму та інших економічинх злочинів, очевидно, що криптовалюти мають певні технічні й концептуальні особливості, що створюють позитивні стимули для їх використанню у злочинній діяльності. Пропонуємо охарактеризувати основні з них.

1. Низький рівень державного регулювання: у більшості країн державні інституції не мають уповноважень для контролю майнінгу й обігу криптовалют, створення й ідентифікації облікових записів пов'язаних з ними, вилучення цифрових активів отриманих незаконним шляхом тощо, що створює позитивні економічні стимули для використання криптовалют для економічної злочинності.

2. Труднощі ідентифікації учасників транзакцій: хоча блокчейн містить публічний запис кожної транзакції, обробленої мережею, ідентифікувати залучених сторін без додаткової інформації (яку можуть надати біржі або інтернет магазини) часто є неможливим (Brenig et al., 2015), також ідентифікація осіб задіяних у транзакції ускладнюється можливістю створення кількох облікових записів однією особою, усе це збільшує анонімність використання криптовалют і зменшує ризики отримання відповідальності за їх використання у злочинній діяльності.

3. Простота конвертації: здатність легко конвертувати криптовалюти у фіатні валюти й навпаки полегшує злочинцям відмивання незаконно здобутих

доходів, уникаючи їх виявлення правоохоронними органами і видаючи за законно здобуті кошти.

4. Доступність: доступність і простота використання криптовалют можуть створити стимул для використання їх як інструменту економічних злочинів, оскільки вони забезпечують ефективний спосіб передачі цінностей через кордони країн без потреби в посередниках або державного нагляду, виключно за наявності пристрою з доступом до Інтернету.

5. Швидкість і низька вартість транзакцій: транзакції фіатних валют зазвичай передбачають високі комісії та значні витрати часу, що робить переміщення великих сум грошей більш складним і дорогим, в той час, як криптовалюти пропонують майже миттєвий час обробки транзакцій, комісії за які є відносно низькими або відсутніми, що робить їх більш привабливим варіантом для економічних злочинців.

6. Безвідкличність: після підтвердження криптовалютної транзакції протокол не пропонує жодних функціональних можливостей для її скасування і повернення стягнених коштів, ця схожість крипитовалютних операцій з готівковими робить їх зручним інструментом для шахрайства.

7. Можливість здійснення платежів без посередника: здійснення транзакціїї з використанням криптовалюти не має необхідності у взаємодії з третіми сторонами для обробки транзакцій (Gowda & Chakravorty, 2021), що робить криптовалютні транзакції значно менш прозорими та контрольованими фінансовими інституціями, державою й громадськістю, а також ускладнює для правоохоронних органів виявлення та відстеження злочинної діяльності.

Не зважаючи на значну кількість позитивних стимулів, що сприяють використанню криптовалют в незаконній діяльності, деякі їх характеристики навпаки роблять криптовалюти менш привабливим інструментом для використання в економічній злочинності. Такими характеристиками можуть бути:

1. Низька ліквідність: хоча все більше продавців пропонують криптовалюти як спосіб оплати за реальні і цифрові товари та послуги, проте криптовалюти все ще є значно менш ліквідними за національні валюти, що обмежує шляхи використання коштів здобутих незаконним шляхом і створює необхідність обміну криптовалют на фіатні валюти.

2. Висока волатильність: криптовалюти відомі своєю мінливістю цін (Baur & Dimpfl, 2021), така нестабільність може ускладнити злочинцям збереження вартості коштів здобутих незаконним шляхом та підвищити ризик фінансових втрат, таким чином, висока волатильність, характерна для криптовалют, є несприятливим фактором для їх використання в економічних злочинах.

3. Запис транзакцій у публічній книзі блокчейну: криптовалюти використовують публічні книги, які реєструють усі транзакції та є видимими

для всіх користувачів, що робить можливим відстеження потенційно злочинних транзакцій, а також дій ідентифікованих злочинних акаунтів правоохоронними органами (Morishima & Matsutani, 2019), що полегшує відстеження злочинної діяльності.

4. Необхідність наявності технічних знань: самостійне використання криптовалют вимагає від злочинців наявності певного рівня технічних знань і навичок, що може стати перешкодою для використання криптовалют, як інструменту економічних злочинів окремими особами.

Підсумовуючи, незважаючи на труднощі з виявленням і ідентифікацією злочинців, наявні оцінки свідчать про загальну тенденцію до зростання участі криптовалют у економічній злочинній діяльності протягом 2017-2022 років. У дослідженні було сформульовано та охарактеризовано основні технічні та концептуальні позитивні стимули до використання криптовалют у економічній злочинності. Також виявлено і розглянуто фактори, що є негативними стимулами до використання криптовалют у економічній злочинності. Результати роботи дозволяють розуміти сприятливі та несприятливі для залучення до економічної злочинності характеристики криптовалют, що може бути використаним для подальшого вивчення та розробки системи державного регулювання цифрових активів, яка покликана запобігати злочинній діяльності та створювати безпечне інвестиційне середовище шляхом, що мінімально заважатиме розвитку інновацій та зростанню галузі цифрових активів.

Список літератури

1. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). NISTIR 8202. *Blockchain Technology Overview*. National Institute of Standards and Technology.

2. Grauer, K., Jardine, E., Leosz, E., & Updegrave, H. (2023). *The 2023 crypto crime report*. Chainalysis.

3. Brenig, C., Accorsi, R., & Müller, G. (2015). Economic Analysis of Cryptocurrency Backed Money Laundering. ECIS 2015 *Completed Research Papers*, Paper 20.

4. Gowda, N., & Chakravorty, C. (2021). Comparative study on cryptocurrency transaction and banking transaction. *Global Transitions Proceedings*, 2(2), 530–534.

5. Baur, D. G., & Dimpfl, T. (2021). The volatility of Bitcoin and its role as a medium of exchange and a store of value. *Empirical Economics*, 61, 2663–2683.

6. Morishima, S., & Matsutani, H. (2019). Acceleration of anomaly detection in blockchain using in-gpu cache. *2018 IEEE intl conf on parallel & distributed processing with applications, ubiquitous computing & communications, big data & cloud computing, social computing & networking, sustainable computing & communications*. IEEE.